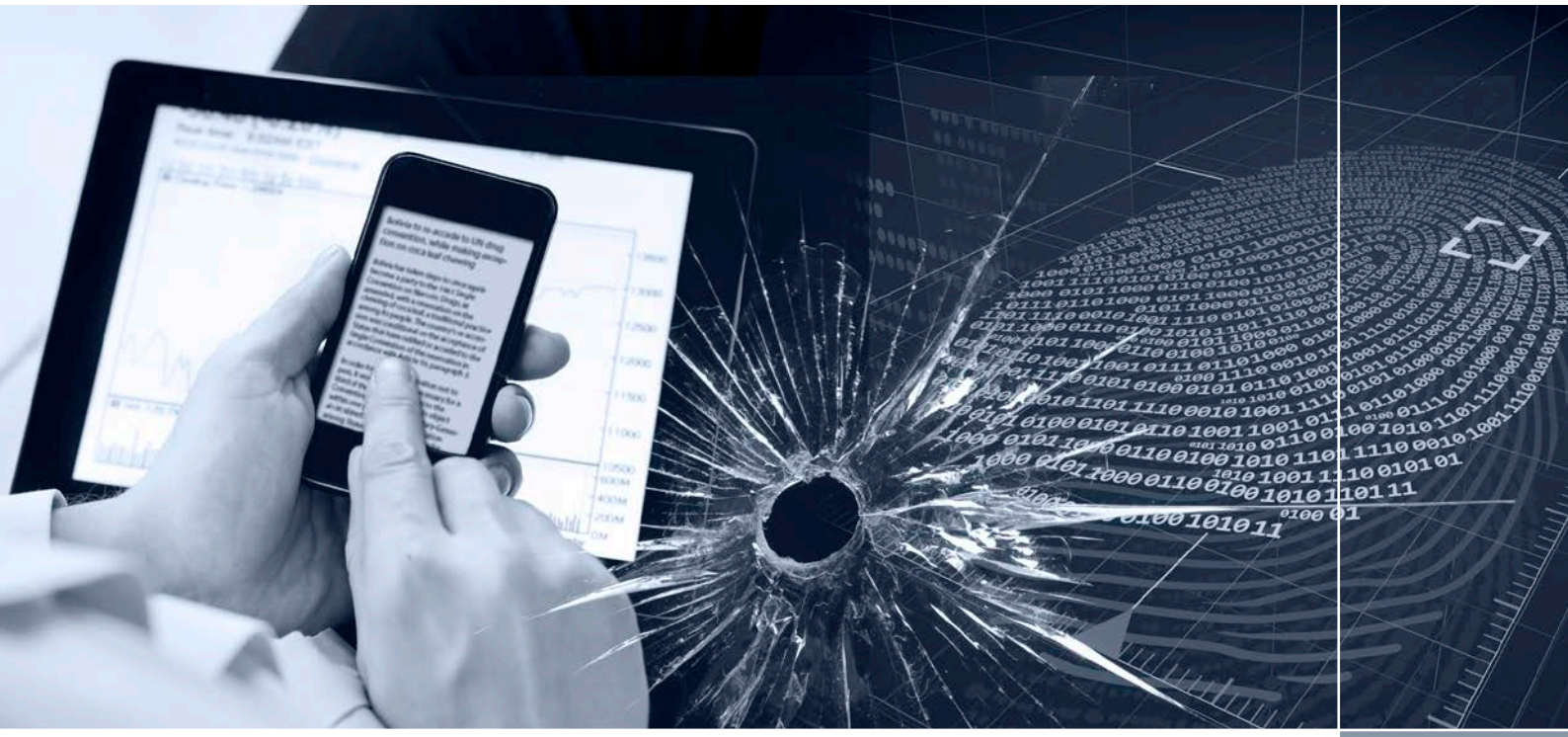
UNODC
United Nations Office on Drugs and Crime



Comprehensive Study on Cybercrime

February 2013

Front cover photo credits (left to right):
©iStockphoto.com/TommL
©iStockphoto.com/mikewesson
©iStockphoto.com/polygraphus

UNITED NATIONS OFFICE ON DRUGS AND CRIME
Vienna

Comprehensive Study on Cybercrime

February 2013

UNITED NATIONS
New York, 2013

© United Nations, February 2013. All rights reserved worldwide.

ACKNOWLEDGEMENTS

This report was prepared for the open-ended intergovernmental expert group on cybercrime by Conference Support Section, Organized Crime Branch, Division for Treaty Affairs, UNODC, under the supervision of John Sandage (Director, Division for Treaty Affairs), Sara Greenblatt (Chief, Organized Crime Branch), and Gillian Murray (UNODC Senior Focal Point for Cybercrime and Chief, Conference Support Section).

Study team:

Steven Malby, Robyn Mace, Anika Holterhof, Cameron Brown, Stefan Kascherus, Eva Ignatuschtschenko (UNODC)

Consultants:

Ulrich Sieber, Tatiana Tropina, Nicolas von zur Mühlen
(Max Planck Institute for Foreign and International Criminal Law)

Ian Brown, Joss Wright
(Oxford Internet Institute and Cyber Security Centre, University of Oxford)

Roderic Broadhurst
(Australian National University)

Kristin Krüger
(Brandenburg Institute for Society and Security)

DISCLAIMERS

This report was prepared for the second meeting of the open-ended intergovernmental expert group on cybercrime. This report has not been formally edited and remains subject to editorial changes.

The contents of this report do not necessarily reflect the views or policies of UNODC or contributory organizations and neither do they imply any endorsement.

The designations employed and the presentation of material in this report do not imply the expression of any opinion whatsoever on the part of UNODC concerning the legal status of any county, territory or city or its authorities, or concerning the delimitation of its frontiers and boundaries.

CONTENTS

ABBREVIATIONS v
INTRODUCTION ix
KEY FINDINGS AND OPTIONS xi
EXECUTIVE SUMMARY xvii

CHAPTER ONE: CONNECTIVITY AND CYBERCRIME **1**
1.1. The global connectivity revolution 1
1.2. Contemporary cybercrime 4
1.3. Cybercrime as a growing challenge 6
1.4. Describing cybercrime 11

CHAPTER TWO: THE GLOBAL PICTURE **23**
2.1. Measuring cybercrime 23
2.2. The global cybercrime picture 25
2.3. Cybercrime perpetrators 39

CHAPTER THREE: LEGISLATION AND FRAMEWORKS **51**
3.1. Introduction – The role of law 51
3.2. Divergence and harmonization of laws 56
3.3. Overview of international and regional instruments 63
3.4. Implementing multilateral instruments at the national level 72

CHAPTER FOUR: CRIMINALIZATION **77**
4.1. Criminalization overview 77
4.2. Analysis of specific offenses 81
4.3. International human rights law and criminalization 107

CHAPTER FIVE: LAW ENFORCEMENT AND INVESTIGATIONS .. 117

5.1. Law enforcement and cybercrime 117
5.2. Investigative powers overview 122
5.3. Privacy and investigative measures 134
5.4. Use of investigative measures in practice 142
5.5. Investigations and the private sector 144
5.6. Law enforcement capacity 152

CHAPTER SIX: ELECTRONIC EVIDENCE AND CRIMINAL JUSTICE 157

6.1. Introduction to electronic evidence and digital forensics 157
6.2. Capacity for digital forensics and electronic evidence handling 162
6.3. Cybercrime and the criminal justice system 168
6.4. Criminal justice capacity 172
6.5. Capacity building and technical assistance 178

CHAPTER SEVEN: INTERNATIONAL COOPERATION 183

7.1. Sovereignty, jurisdiction and international cooperation 183
7.2. Jurisdiction 189
7.3. International cooperation I – formal cooperation 197
7.4. International cooperation II – informal cooperation 208
7.5. Extra-territorial evidence from clouds and service providers 216

CHAPTER EIGHT: PREVENTION 225

8.1. Cybercrime prevention and national strategies 225
8.2. Cybercrime awareness 234
8.3. Cybercrime prevention, the private sector and academia 239

ANNEX ONE: ACT DESCRIPTIONS 257
ANNEX TWO: MEASURING CYBERCRIME 259
ANNEX THREE: PROVISIONS OF INTERNATIONAL AND REGIONAL INSTRUMENTS 267
ANNEX FOUR: THE INTERNET 277
ANNEX FIVE: METHODOLOGY 283

LIST OF ABBREVIATIONS

Abbreviations

CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
ECHR	European Convention for the Protection of Human Rights and Fundamental Freedoms
ECtHR	European Court of Human Rights
EU	European Union
EUROPOL	European Police Office
G8	Group of Eight
GDP	Gross domestic product
HDI	Human Development Index
ICCPR	International Covenant on Civil and Political Rights
ICCPR-OP2	Second Optional Protocol to the International Covenant on Civil and Political Rights, aiming at the abolition of the death penalty
ICERD	International Convention on the Elimination of All Forms of Racial Discrimination
ICESCR	International Covenant on Economic, Social and Cultural Rights
ICRMW	United Nations International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families
ICT	Information and communications technology
INTERPOL	International Criminal Police Organization
IP	Internet protocol
ISP	Internet service provider
IT	Information technology
ITU	International Telecommunication Union
NFC	Near field communication
OP-CRC-SC	Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography
P2P	Peer-to-peer
SCO	Shanghai Cooperation Organisation
SMS	Short message service
TRIPS	Agreement on Trade Related Aspects of Intellectual Property Rights
UNESCO	United Nations Educational, Scientific and Cultural Organization
UNODC	United Nations Office on Drugs and Crime
UNSC	United Nations Security Council
URL	Uniform Resource Locator
USB	Universal serial bus
VGT	Virtual global taskforce
WEF	World Economic Forum

African Union, 2012. Draft Convention on the Establishment of a Legal Framework Conductive to Cybersecurity in Africa (**Draft African Union Convention**).

Common Market for Eastern and Southern Africa (COMESA), 2011. Cybersecurity Draft Model Bill. (**COMESA Draft Model Bill**).

The Commonwealth, 2002. (i) Computer and Computer Related Crimes Bill and (ii) Model Law on Electronic Evidence (**Commonwealth Model Law**).

Commonwealth of Independent States, 2001. Agreement on Cooperation in Combating Offences related to Computer Information (**Commonwealth of Independent States Agreement**).

Council of Europe, 2001. Convention on Cybercrime and Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (**Council of Europe Cybercrime Convention/Protocol**).

Council of Europe, 2007. Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (**Council of Europe Child Protection Convention**).

Economic Community of West African States (ECOWAS), 2009. Draft Directive on Fighting Cybercrime within ECOWAS (**ECOWAS Draft Directive**).

European Union, 2000. Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (**EU Directive on e-Commerce**).

European Union, 2001. Council Framework Decision 2001/413/JHA combating fraud and counterfeiting of non-cash means of payment (**EU Decision on Fraud and Counterfeiting**).

European Union, 2002. Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector (**EU Directive on Data Protection**).

European Union, 2005. Council Framework Decision 2005/222/JHA on attacks against information systems (**EU Decision on Attacks against Information Systems**).

European Union, 2006. Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks (**EU Directive on Data Retention**).

European Union, 2010. Proposal COM(2010) 517 final for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA (**EU Directive Proposal on Attacks against Information Systems**).

European Union, 2011. Directive 2011/92/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (**EU Directive on Child Exploitation**).

International Telecommunication Union (ITU)/Caribbean Community (CARICOM)/Caribbean Telecommunications Union (CTU), 2010. Model Legislative Texts on Cybercrime/e-Crimes

and Electronic Evidence (**ITU/CARICOM/CTU Model Legislative Texts**).

League of Arab States, 2010. Arab Convention on Combating Information Technology Offences (**League of Arab States Convention**).

League of Arab States, 2004. Model Arab Law on Combating Offences related to Information Technology Systems (**League of Arab States Model Law**).

Shanghai Cooperation Organization, 2010. Agreement on Cooperation in the Field of International Information Security (**Shanghai Cooperation Organization Agreement**).

United Nations, 2000. Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography (**United Nations OP-CRC-SC**).

Page left intentionally blank

INTRODUCTION

General Assembly resolution 65/230 requested the Commission on Crime Prevention and Criminal Justice to establish an open-ended intergovernmental expert group, to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation.

In its resolution 65/230, the General Assembly requested the Commission on Crime Prevention and Criminal Justice to establish, in line with paragraph 42 of the Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, an open-ended intergovernmental expert group, to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.[1]

In its resolution 67/189, the General Assembly noted with appreciation the work of the open-ended intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime and encouraged it to enhance its efforts to complete its work and to present the outcome of the study to the Commission on Crime Prevention and Criminal Justice in due course.

The first session of the expert group was held in Vienna from 17 to 21 January 2011. At that meeting, the expert group reviewed and adopted a collection of topics and a methodology for the study.[2]

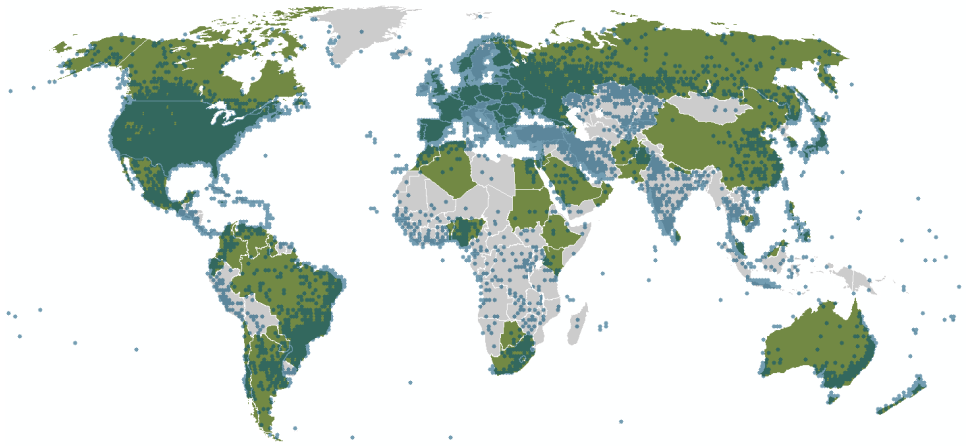
The collection of topics for consideration within a comprehensive study on cybercrime included the problem of cybercrime, legal responses to cybercrime, crime prevention and criminal justice capabilities and other responses to cybercrime, international organizations, and technical assistance. These main topics were further divided into 12 sub-topics.[3] Within this Study, these topics are covered in eight Chapters: (1) Connectivity and cybercrime; (2) The global picture; (3) Legislation and frameworks; (4) Criminalization; (5) Law enforcement and investigations; (6) Electronic evidence and criminal justice; (7) International cooperation; and (8) Prevention.

The methodology for the study tasked the United Nations Office on Drugs and Crime with developing the study, including developing a questionnaire for the purposes of information gathering, collecting and analyzing data, and developing a draft text of the study. Information gathering in accordance with the methodology, including the distribution of a questionnaire to Member States, intergovernmental organizations and representatives from the private sector and

1 General Assembly resolution 65/230, Annex.
2 E/CN.15/2011/19
3 (1) Phenomenon of cybercrime; (2) Statistical information; (3) Challenges of cybercrime; (4) Common approaches to legislation; (5) Criminalization; (6) Procedural powers; (7) International cooperation; (8) Electronic evidence; (9) Roles and responsibilities of service providers and the private sector; (10) Crime prevention and criminal justice capabilities and other responses to cybercrime; (11) International organizations; and (12) Technical assistance.

academic institutions, was conducted by UNODC, from February 2012 to July 2012. Information was received from 69 Member States with regional distribution as follows: Africa (11), Americas (13), Asia (19), Europe (24), and Oceania (2). Information was received from 40 private sector organizations, 16 academic organizations and 11 intergovernmental organizations. Over 500 open-source documents were also reviewed by the Secretariat. Further details on the methodology are contained at Annex Five to this Study.

Member State responses to the Study questionnaire (green) and Internet penetration (blue)



Source: Study questionnaire responses and UNODC elaboration of MaxMind GeoCityLite

As required by General Assembly resolution 65/230, this Study has been prepared with a view to 'examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.' The mandate comes within the context of a number of other mandates and activities related to cybercrime and cybersecurity within the United Nations system.[4] In this respect, the focus of the Study is limited to the *crime prevention* and *criminal justice* aspects of preventing and combating cybercrime.

The Study represents a 'snapshot' in time of crime prevention and criminal justice efforts to prevent and combat cybercrime.

It paints a global picture, highlighting lessons learned from current and past efforts, and presenting possible options for future responses. While the Study is, by title, a study on 'cybercrime', it has unique relevance for *all* crimes. As the world moves into a hyper-connected society with universal internet access, it is hard to imagine a 'computer crime', and perhaps any crime, that will not involve electronic evidence linked with internet connectivity. Such developments may well require fundamental changes in law enforcement approach, evidence gathering, and mechanisms of international cooperation in criminal matters.

[4] Including work in the context of developments in the field of information and telecommunications in the context of international security. See A/RES/66/24.

KEY FINDINGS AND OPTIONS

General Assembly resolution 65/230 requested the intergovernmental expert group to conduct a comprehensive study of the problem of cybercrime with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime. This Part presents the key findings from the Study together with such options.

Key findings

- The key findings from the Study concern issues of:
  - the impact of fragmentation at international level and diversity of national cybercrime laws on international cooperation
  - a reliance on traditional means of formal international cooperation in criminal matters involving cybercrime and electronic evidence for all crimes
  - the role of evidence 'location'
  - harmonization of national legal frameworks
  - law enforcement and criminal justice capacity
  - cybercrime prevention activities

The Study examined the problem of cybercrime from the perspective of governments, the private sector, academia and international organizations. The results are presented in eight Chapters, covering internet connectivity and cybercrime; the global cybercrime picture; cybercrime legislation and frameworks; criminalization of cybercrime; law enforcement and cybercrime investigations; electronic evidence and criminal justice; international cooperation in criminal matters involving cybercrime; and cybercrime prevention.

Key findings in these areas are presented below and further expanded upon in the Executive summary that follows this Part:

(a) Fragmentation at the international level, and diversity of national cybercrime laws, may correlate with the existence of multiple instruments with different thematic and geographic scope. While instruments legitimately reflect socio-cultural and regional differences, divergences in the extent of procedural powers and international cooperation provisions may lead to the emergence of country cooperation 'clusters' that are not always well suited to the global nature of cybercrime;

(b) Reliance on traditional means of formal international cooperation in cybercrime matters is not currently able to offer the timely response needed for obtaining volatile electronic evidence. As an increasing number of crimes involve geo-distributed electronic evidence, this will become an issue not only for cybercrime, but all crimes in general;

(c) In a world of cloud computing and data centres, the role of evidence 'location' needs to be reconceptualized, including with a view to obtaining consensus on issues concerning direct access to extraterritorial data by law enforcement authorities;

(d) Analysis of available national legal frameworks indicates insufficient harmonization of 'core' cybercrime offences, investigative powers, and admissibility of electronic evidence. International human rights law represents an important external reference point for criminalization and procedural provisions;

(e) Law enforcement authorities, prosecutors, and judiciary in developing countries, require long-term, sustainable, comprehensive technical support and assistance for the investigation and combating of cybercrime;

(f) Cybercrime prevention activities in all countries require strengthening, through a holistic approach involving further awareness raising, public-private partnerships, and the integration of cybercrime strategies with a broader cybersecurity perspective.

Options to strengthen existing and to propose new national and international legal or other responses to cybercrime

- Options to strengthen existing and to propose new national and international legal or other responses to cybercrime include:
  - Development of international model provisions
  - Development of a multilateral instrument on international cooperation regarding electronic evidence in criminal matters
  - Development of a comprehensive multilateral instrument on cybercrime
  - Delivery of enhanced technical assistance for the prevention and combating of cybercrime in developing countries

The options presented are informed by responses of countries to a question in the Study questionnaire regarding options that should be considered to strengthen existing and to propose new national and international legal or other responses to cybercrime, as well as by the key findings.

In response to this question, countries proposed a range of possibilities. The majority of options suggested related to areas such as: harmonization of laws; accession to existing international or regional cybercrime instruments; the development of new international legal instruments; strengthening mechanisms for international cooperation and obtaining of extraterritorial evidence in practice; and capacity building for law enforcement and criminal justice institutions.[1]

Many countries highlighted that an expedited mechanism for international cooperation procedures in criminal matters involving cybercrime should be developed. Some countries proposed that this could be through the strengthening of existing informal police-to-police networks. Other countries proposed that this could be achieved by further development of existing formal international cooperation channels, including bilateral and multilateral agreements. Some countries emphasized that all options should be implemented in line with international human rights standards, including rights to freedom of expression and to privacy.

[1] Study cybercrime questionnaire. Q11.

Some countries recommended that accession to the Council of Europe Cybercrime Convention would promote international cooperation and harmonization of national cybercrime laws. Some countries recommended that a new international legal instrument on cybercrime should be developed. Other countries recommended that harmonization of legislation could be promoted through the development of international model legal provisions at the United Nations level.

A number of countries recommended that international standards should be developed on law enforcement investigations concerning extraterritorial data, including with a view to clarifying the relationship of such investigations with national sovereignty principles.

A number of countries suggested that technical assistance for law enforcement, prosecutorial and judicial authorities in the area of preventing and combating cybercrime should be strengthened.

On the basis of proposals made by Member States and the key findings, the Study finds that options to strengthen existing and to propose new national and international legal or other responses to cybercrime may include one or more of the following:

(a) The development of international model provisions on criminalization of core cybercrime acts, with a view to supporting States in eliminating safe havens through the adoption of common offence elements:

(i) The provisions could maintain the approach of existing instruments regarding offences against the confidentiality, integrity and accessibility of computer systems and data;

(ii) The provisions could also cover 'conventional' offences perpetrated or facilitated by use of computer systems, only where existing criminalization approaches are perceived not to be sufficient;

(iii) The provisions could address areas not covered by existing instruments, such as criminalization of SPAM;

(iv) The provisions could be developed in line with the latest international human rights standards on criminalization, including in particular, treaty-based protections of the right to freedom of expression;

(v) Use of the provisions by States would minimize dual criminality challenges in international cooperation;

(b) The development of international model provisions on investigative powers for electronic evidence, with a view to supporting States in ensuring the necessary procedural tools for investigation of crimes involving electronic evidence:

(i) The provisions could draw on the approach of existing instruments, including orders for expedited preservation of data, and orders for obtaining stored and real-time data;

(ii) The provisions could offer guidance on the extension of traditional powers such as search and seizure to electronic evidence;

(iii) The provisions could offer guidance on the application of appropriate safeguards for intrusive investigative techniques based on international human rights law, including treaty-based protections of the right to privacy;

(c) The development of model provisions on jurisdiction, in order to provide for common effective bases for jurisdiction in cybercrime criminal matters:

(i) The provisions could include bases such as those derived from the objective territoriality principle and the substantial effects doctrine.

(ii) The provisions could include guidance for addressing issues of concurrent jurisdiction.

(d) The development of model provisions on international cooperation regarding electronic evidence, for inclusion in bilateral or multilateral instruments, including a revised United Nations Model Treaty on Mutual Legal Assistance, in line with suggestions in the Discussion Guide for the Thirteenth Congress on Crime Prevention and Criminal Justice:

(i) The provisions would focus on practical cooperation mechanisms that could be inserted in existing instruments for the timely preservation and supply of electronic evidence in criminal matters;

(ii) The provisions could include obligations to establish electronic evidence fast response focal points and agreed timescales for responses;

(e) The development of a multilateral instrument on international cooperation regarding electronic evidence in criminal matters, with a view to providing an international mechanism for timely cooperation to preserve and obtain electronic evidence:

(i) By way of complementarity to existing international cooperation treaties, such an instrument could focus primarily on a mechanism for requesting expedited preservation of data for a specified time period;

(ii) The instrument may also include specific cooperation provisions for further investigative measures, including supply of stored data, and real-time collection of data;

(iii) The scope of application would need to be defined, but should not be limited to 'cybercrime' or 'computer-related' crime;

(iv) The instrument could require response within a specified time period and establish clear focal point to focal point communication channels, building upon rather than duplicating existing 24/7 initiatives;

(v) The instrument could include traditional international cooperation safeguards, as well as appropriate human rights exclusions;

(f) The development of a comprehensive multilateral instrument on cybercrime, with a view to establishing an international approach in the areas of criminalization, procedural powers, jurisdiction, and international cooperation:

(i) The instrument could include elements from all of the options above in a binding, multilateral form;

(ii) The instrument could draw on existing core commonalities across the current range of binding and non-binding international and regional instruments;

(g) The strengthening of international, regional and national partnerships, including with the private sector and academic institutions, with a view to delivering enhanced technical assistance for the prevention and combating of cybercrime in developing countries:

(i) Technical assistance could be delivered based on standards developed through model provisions as set out in the options above;

(ii) Technical assistance could be delivered through a focus on multi-stakeholder delivery, including representatives from the private sector and academia.

Page left intentionally blank

EXECUTIVE SUMMARY

Connectivity and cybercrime

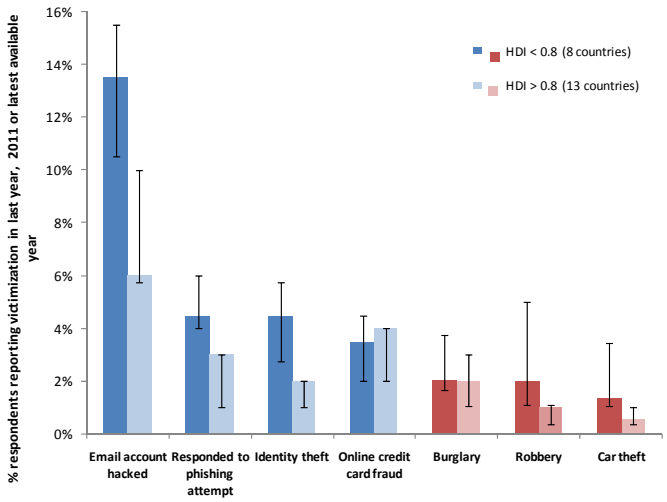
In 2011, at least 2.3 billion people, the equivalent of more than one third of the world's total population, had access to the internet. Over 60 per cent of all internet users are in developing countries, with 45 per cent of all internet users below the age of 25 years. By the year 2017, it is estimated that mobile broadband subscriptions will approach 70 per cent of the world's total population. By the year 2020, the number of networked devices (the 'internet of things') will outnumber people by six to one, transforming current conceptions of the internet. In the hyperconnected world of tomorrow, it will become hard to imagine a 'computer crime', and perhaps any crime, that does not involve electronic evidence linked with internet protocol (IP) connectivity.

'Definitions' of cybercrime mostly depend upon the purpose of using the term. A limited number of acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime. Beyond this, however, computer-related acts for personal or financial gain or harm, including forms of identity-related crime, and computer content-related acts (all of which fall within a wider meaning of the term 'cybercrime') do not lend themselves easily to efforts to arrive at legal definitions of the aggregate term. Certain definitions are required for the core of cybercrime acts. However, a 'definition' of cybercrime is not as relevant for other purposes, such as defining the scope of specialized investigative and international cooperation powers, which are better focused on electronic evidence for any crime, rather than a broad, artificial 'cybercrime' construct.

The global picture

In many countries, the explosion in global connectivity has come at a time of economic and demographic transformations, with rising income disparities, tightened private sector spending, and reduced financial liquidity. At the global level, law enforcement respondents to the study perceive increasing levels of cybercrime, as both individuals and organized criminal groups exploit new criminal opportunities, driven by profit and personal gain. Upwards of 80 per cent of cybercrime acts are estimated to originate in some form of organized activity, with cybercrime black markets established on a cycle of malware creation, computer infection, botnet management, harvesting of personal and financial data, data sale, and 'cashing out' of financial information. Cybercrime perpetrators no longer require complex skills or techniques. In the developing country context in particular, sub-cultures of young men engaged in computer-related financial fraud have emerged,

Cybercrime and conventional crime victimization



Source: UNODC elaboration of Norton Cybercrime Report and crime victimization surveys.

many of whom begin involvement in cybercrime in late teenage years.

Globally, cybercrime acts show a broad distribution across financial-driven acts, and computer-content related acts, as well as acts against the confidentiality, integrity and accessibility of computer systems. Perceptions of relative risk and threat vary, however, between Governments and private sector enterprises. Currently, police-recorded crime statistics do not represent a sound basis for cross-national comparisons, although such statistics are often important for policy making at the national level. Two-thirds of countries view their systems of police statistics as insufficient for recording cybercrime. Police-recorded cybercrime rates are associated with levels of country development and specialized police capacity, rather than underlying crime rates.

Victimization surveys represent a more sound basis for comparison. These demonstrate that individual cybercrime victimization is significantly higher than for 'conventional' crime forms. Victimization rates for online credit card fraud, identity theft, responding to a phishing attempt, and experiencing unauthorized access to an email account, vary between 1 and 17 per cent of the online population for 21 countries across the world, compared with typical burglary, robbery and car theft rates of under 5 per cent for these same countries. Cybercrime victimization rates are higher in countries with lower levels of development, highlighting a need to strengthen prevention efforts in these countries.

Private sector enterprises in Europe report similar victimization rates – between 2 and 16 per cent – for acts such as data breach due to intrusion or phishing. Criminal tools of choice for these crimes, such as botnets, have global reach. More than one million unique IP addresses globally functioned as botnet command and control servers in 2011. Internet content also represented a significant concern for Governments. Material targeted for removal includes child pornography and hate speech, but also content related to defamation and government criticism, raising human rights law concerns in some cases. Almost 24 per cent of total global internet traffic is estimated to infringe copyright, with downloads of shared peer-to-peer (P2P) material particularly high in countries in Africa, South America, and Western and South Asia.

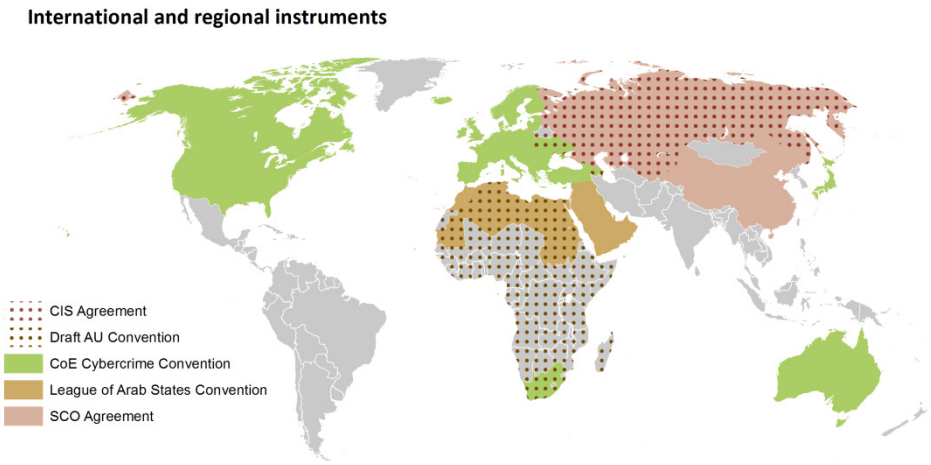
Legislation and frameworks

Legal measures play a key role in the prevention and combating of cybercrime. These are required in all areas, including criminalization, procedural powers, jurisdiction, international cooperation, and internet service provider responsibility and liability. At the national level, both existing and new (or planned), cybercrime laws most often concern criminalization, indicating a predominant focus on establishing specialized offences for core cybercrime acts. Countries increasingly recognize, however, the need for legislation in other areas. Compared to existing laws, new or planned cybercrime laws more frequently address investigative measures, jurisdiction, electronic evidence and international cooperation. Globally, less than half of responding countries perceive their criminal and procedural law frameworks to be sufficient, although this masks large regional differences. While more than two-thirds of countries in Europe report sufficient legislation, the picture is reversed in Africa, the Americas, Asia and Oceania, where more than two-thirds of countries view laws as only partly sufficient, or not sufficient at all. Only one half of the countries, which reported that laws were insufficient, also indicated new or planned laws, thus highlighting an urgent need for legislative strengthening in these regions.

The last decade has seen significant developments in the promulgation of international and regional instruments aimed at countering cybercrime. These include binding and non-binding instruments. Five clusters can be identified, consisting of instruments developed in the context of, or

inspired by: (i) the Council of Europe or the European Union, (ii) the Commonwealth of Independent States or the Shanghai Cooperation Organization, (iii) intergovernmental African organizations, (iv) the League of Arab States, and (v) the United Nations. A significant amount of cross-fertilization exists between all instruments, including, in particular, concepts and approaches developed in the Council of Europe Convention on Cybercrime. Analysis of the articles of 19 multilateral instruments relevant to cybercrime shows common core provisions, but also significant divergence in substantive areas addressed.

Globally, 82 countries have signed and/or ratified a binding cybercrime instrument.[1] In addition to formal membership and implementation, multilateral cybercrime instruments have influenced national laws indirectly, through use as a model by non-States parties, or via the influence of legislation of States parties on other countries. Membership of a multilateral cybercrime instrument corresponds with the perception of increased sufficiency of national criminal and procedural law, indicating that current multilateral provisions in these areas are generally considered effective. For the more than 40 countries that provided information, the Council of Europe Convention on Cybercrime is the most used multilateral instrument for the development of cybercrime legislation. Altogether, multilateral instruments from other 'clusters' were used in around half as many countries.



Overall, one-third of responding countries report that their legislation is highly, or very highly, harmonized with countries viewed as important for the purposes of international cooperation. This varies regionally, however, with higher degrees of harmonization reported within the Americas and Europe. This may be due to the use, in some regions, of multilateral instruments, which are inherently designed to play a role in harmonization. Fragmentation at the international level, and diversity of national laws, in terms of cybercrime acts criminalized, jurisdictional bases, and mechanisms of cooperation, may correlate with the existence of multiple cybercrime instruments with different thematic and geographic scope. Both instruments and regions presently reflect divergences derived from underlying legal and constitutional differences, including differing conceptions of rights and privacy.

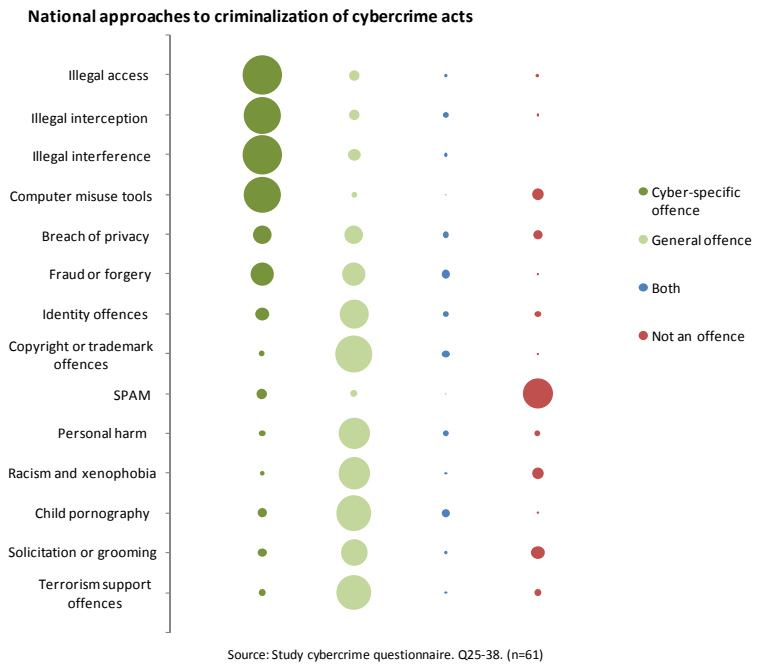
Criminalization

Information on cybercrime criminal laws was gathered through the study questionnaire, as well as by primary source analysis of available legislation collected by the Secretariat.[2] The study

[1] One or more of: The Council of Europe Convention on Cybercrime, the League of Arab States Convention on Combating Information Technology Offences, the Commonwealth of Independent States Agreement on Cooperation in Combating Offences related to Computer Information, or the Shanghai Cooperation Organization Agreement in the Field of International Information Security.

[2] Primary source legislation was analyzed for 97 Member States, including 56 that responded to the questionnaire, with regional distribution as follows: Africa (15), Americas (22), Asia (24), Europe (30), and Oceania (6).

questionnaire referred to 14 acts commonly included in notions of cybercrime.[3] Responding countries described widespread criminalization of these 14 acts, with the primary exception of SPAM offences and, to some extent, offences concerning computer misuse tools, racism and xenophobia, and online solicitation or 'grooming' of children. This reflects a certain baseline consensus on culpable cybercrime conduct. Countries reported few additional crimes, not mentioned in the questionnaire. These mostly concerned computer content, including criminalization of obscene material, online gambling, and online illicit markets, such as in drugs and persons. For the 14 acts, countries reported the use of cyber-specific offences for core cybercrime acts against the confidentiality, integrity and accessibility of computer systems. For other forms of cybercrime, general (non-cyber-specific) offences were used more often. Both approaches were reported, however, for computer-related acts involving breach of privacy, fraud or forgery, and identity offences.



Source: Study cybercrime questionnaire. Q25-38. (n=61)

While high-level consensus exists regarding broad areas of criminalization, detailed analysis of the provisions in source legislation reveals divergent approaches. Offences involving illegal *access* to computer systems and data differ with respect to the object of the offence (data, system, or information), and regarding the criminalization of 'mere' access or the requirement for further intent, such as to cause loss or damage. The requisite intent for an offence also differs in approaches to criminalization of *interference* with computer systems or data. Most countries require the interference to be intentional, while others include reckless interference. For interference with computer data, the conduct constituting interference ranges from damaging or deleting, to altering, suppressing, inputting or transmitting data. Criminalization of illegal *interception* differs by virtue of whether the offence is restricted to non-public data transmissions or not, and concerning whether the crime is restricted to interception 'by technical means'. Not all countries criminalize *computer misuse tools*. For those that do, differences arise regarding whether the offence covers possession, dissemination, or use of software (such as malware) and/or computer access codes (such as victim passwords). From the perspective of international cooperation, such differences may have an impact upon findings of dual-criminality between countries.

Several countries have adopted cyber-specific crimes for computer-related fraud, forgery and identity offences. Others extend general provisions on fraud or theft, or rely on crimes covering

[3] Illegal access to a computer system; illegal access, interception or acquisition of computer data; illegal data interference or system interference; production, distribution or possession of computer misuse tools; breach of privacy or data protection measures; computer-related fraud or forgery; computer-related identity offences; computer-related copyright and trademark offences; computer-related acts causing personal harm; computer-related acts involving racism or xenophobia; computer-related production, distribution or possession of child pornography; computer-related solicitation or 'grooming' of children; and computer-related acts in support of terrorism offences.

constituent elements – such as illegal access, data interference and forgery, in the case of identity offences. A number of content-related offences, particularly those concerning child pornography, show widespread criminalization. Differences arise however regarding the definition of 'child', limitations in relation to 'visual' material or exclusion of simulated material, and acts covered. Although the vast majority of countries, for instance, cover production and distribution of child pornography, criminalization of possession and access shows greater variation. For computer-related copyright and trademark infringement, countries most usually reported the application of general criminal offences for acts committed wilfully and on a commercial scale.

The increasing use of social media and user-generated internet content has resulted in regulatory responses from governments, including the use of criminal law, and calls for respect for rights to freedom of expression. Responding countries report varying boundaries to expression, including with respect to defamation, contempt, threats, incitement to hatred, insult to religious feelings, obscene material, and undermining the state. The socio-cultural element of some limitations is reflected not only in national law, but also in multilateral instruments. Some regional cybercrime instruments, for example, contain broad offences regarding the violation of public morals, pornographic material, and religious or family principles or values.

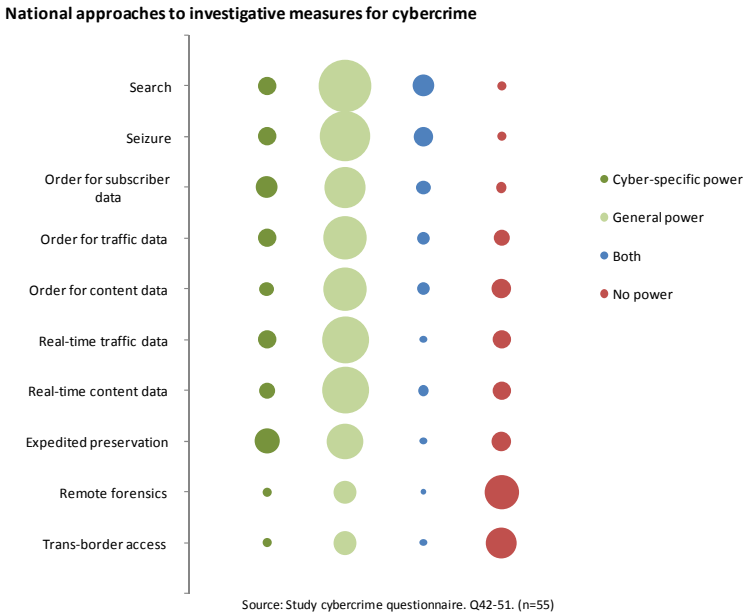
International human rights law acts both as a sword and a shield, requiring criminalization of (limited) extreme forms of expression, while protecting other forms. Some prohibitions on freedom of expression, including incitement to genocide, hatred constituting incitement to discrimination, hostility or violence, incitement to terrorism, and propaganda for war, are therefore required for States that are party to relevant international human rights instruments. For others, the 'margin of appreciation' allows leeway to countries in determining the boundaries of acceptable expression in line with their own cultures and legal traditions. Nonetheless, international human rights law will intervene at a certain point. Penal laws on defamation, disrespect for authority, and insult, for example, that apply to online expressions will face a high threshold of demonstrating that the measures are proportionate, appropriate, and the least intrusive possible. Where content is illegal in one country, but legal to produce and disseminate in another, States will need to focus criminal justice responses on persons accessing content within the national jurisdiction, rather than on content produced outside of the country.

Law enforcement and investigations

Over 90 per cent of responding countries report that cybercrime acts most frequently come to the attention of law enforcement authorities through reports by individual or corporate victims. Responding countries estimate that the proportion of actual cybercrime victimization reported to the police ranges upwards from 1 per cent. One global private sector survey suggests that 80 per cent of individual victims of core cybercrime do not report the crime to the police. Underreporting derives from a lack of awareness of victimization and of reporting mechanisms, victim shame and embarrassment, and perceived reputation risks for corporations. Authorities in all regions of the world highlighted initiatives for increasing reporting, including online and hotline reporting systems, public awareness campaigns, private sector liaison, and enhanced police outreach and information sharing. An incident-driven response to cybercrime must, however, be accompanied by medium and long-term tactical investigations that focus on crime markets and criminal scheme architects. Law enforcement authorities in developed countries are engaged in this area, including through undercover units targeting offenders on social networking sites, chat rooms, and instant messaging and P2P services. Challenges in the investigation of cybercrime arise from criminal innovations by offenders, difficulties in accessing electronic evidence, and from internal resource, capacity and

logistical limitations. Suspects frequently use anonymization and obfuscation technologies, and new techniques quickly make their way to a broad criminal audience through online crime markets.

Law enforcement cybercrime investigations require an amalgamation of traditional and new policing techniques. While some investigative actions can be achieved with traditional powers, many procedural provisions do not translate well from a spatial, object-oriented approach to one involving electronic data storage and real-time data flows. The study questionnaire referred to ten cybercrime investigative measures, ranging from generic search and seizure to specialized powers, such as preservation of computer data.[4] Countries most often reported the existence of general (non-cyber-specific) powers across all investigative measures. A number of countries also reported cyber-specific legislation, notably for ensuring expedited preservation of computer data and obtaining stored subscriber data. Many countries reported a lack of legal power for advanced measures, such as remote computer forensics. While traditional procedural powers can be extended to cyber-situations, in many cases such an approach can also lead to legal uncertainties and challenges to the lawfulness of evidence gathering, and thus the admissibility of evidence. Overall, national approaches to cybercrime investigative powers show less core commonality than for criminalization of many cybercrime acts.



Irrespective of the legal form of investigative powers, all responding authorities use search and seizure for the physical appropriation of computer equipment and the capture of computer data. The majority of countries also use orders for obtaining stored computer data from internet service providers. Outside of Europe, however, around one third of countries report challenges in compelling third parties in an investigation to provide information. Around three-quarters of countries use specialized investigative measures, such as real-time collection of data, or expedited preservation of data. Use of investigative measures typically requires a minimum of initial evidence or a report of a cybercrime act. More intrusive measures, such as those involving real-time collection of data or accessing of data content, often require higher thresholds, such as evidence of a serious act, or demonstration of probable cause or reasonable grounds.

The interplay between law enforcement and internet service providers is particularly complex. Service providers hold subscriber information, billing invoices, some connection logs, location information (such as cell tower data for mobile providers), and communication

[4] Search for computer hardware or data; seizure of computer hardware or data; order for subscriber information; order for stored traffic data; order for stored content data; real-time collection of traffic data; real-time collection of content data; expedited preservation of computer data; use of remote forensic tools; and trans-border access to a computer system or data.

content, all of which can represent critical electronic evidence of an offence. National legal obligations and private sector data retention and disclosure policies vary widely by country, industry and type of data. Countries most often reported using court orders to obtain evidence from service providers. In some cases, however, law enforcement may be able to obtain stored subscriber data, traffic data, and even content data, directly. In this respect, private sector organizations often reported both a primary policy of requiring due legal process for data disclosure, but also voluntary compliance with direct law enforcement requests under some circumstances. Informal relationships between law enforcement and service providers, the existence of which was reported in more than half of all responding countries, assist the process of information exchange and trust-building. Responses indicated that there is a need to balance privacy and due process, with disclosure of evidence in a timely manner, in order to ensure that the private sector does not become a 'choke-point' for investigations.

Cybercrime investigations invariably involve considerations of privacy under international human rights law. Human rights standards specify that laws must be sufficiently clear to give an adequate indication of the circumstances in which authorities are empowered to use an investigative measure, and that adequate and effective guarantees must exist against abuse. Countries reported the protection of privacy rights in national law, as well as a range of limits and safeguards on investigations. When investigations are transnational, divergences in levels of protection, however, give rise to unpredictability regarding foreign law enforcement access to data, and potential jurisdictional gaps in privacy protection regimes.

Over 90 per cent of the countries that responded to the questionnaire have begun to put in place specialized structures for the investigation of cybercrime and crimes involving electronic evidence. In developing countries, however, these are not well resourced and suffer from a capacity shortage. Countries with lower levels of development have significantly fewer specialized police, with around 0.2 per 100,000 national internet users. The rate is two to five times higher in more developed countries. Seventy per cent of specialized law enforcement officers in less developed countries were reported to lack computer skills and equipment, and only half receive training more than once a year. More than half of responding countries in Africa, and one-third of countries in the Americas report that law enforcement resources for investigating cybercrime were insufficient. Globally, it is likely that the picture is worse. The study received responses, for example, from only 20 per cent of the world's 50 least developed countries. All responding countries in Africa, and over 80 per cent of countries in the Americas and Asia and Oceania reported requiring technical assistance. The most commonly cited area for technical assistance required was general cybercrime investigative techniques. Of those countries requiring assistance, 60 per cent indicated that this was needed by law enforcement agencies.

Electronic evidence and criminal justice

Evidence is the means by which facts relevant to the guilt or innocence of an individual at trial are established. Electronic evidence is all such material that exists in electronic, or digital, form. It can be stored or transient. It can exist in the form of computer files, transmissions, logs, metadata, or network data. Digital forensics is concerned with recovering – often volatile and easily contaminated – information that may have evidential value. Forensics techniques include the creation of 'bit-for-bit' copies of stored and deleted information, 'write-blocking' in order to ensure that the original information is not changed, and cryptographic file 'hashes', or digital signatures, that can demonstrate changes in information. Almost all countries reported some digital forensics capacity. Many responding countries, across all

regions, however, note insufficient numbers of forensic examiners, differences between capacity at federal and state level, lack of forensics tools, and backlogs due to overwhelming quantities of data for analysis. One half of countries report that suspects make use of encryption, rendering access to this type of evidence difficult and time-consuming without the decryption key. In most countries, the task of analyzing electronic evidence lies with law enforcement authorities. Prosecutors, however, must view and understand electronic evidence in order to build a case at trial. All countries in Africa and one-third of countries in other regions reported insufficient resources for prosecutors to do so. Prosecution computer skills are typically lower than those of investigators. Globally, around 65 per cent of responding countries report some form of prosecutorial cybercrime specialization. Just 10 per cent of countries report specialized judicial services. The vast majority of cybercrime cases are handled by non-specialized judges, who, in 40 per cent of responding countries, do not receive any form of cybercrime-related training. Judicial training on cybercrime law, evidence collection, and basic and advanced computer knowledge represents a particular priority.

Over 60 per cent of responding countries do not make a legal distinction between electronic evidence and physical evidence. While approaches vary, many countries consider this good practice, as it ensures fair admissibility alongside all other types of evidence. A number of countries outside of Europe do not admit electronic evidence at all, making the prosecution of cybercrime, and any other crime evidenced by electronic information, unfeasible. While countries do not, in general, have separate evidentiary rules for electronic evidence, a number of countries referred to principles such as: the best evidence rule, the relevance of evidence, the hearsay rule, authenticity, and integrity, all of which may have particular application to electronic evidence. Many countries highlighted challenges of attribution of acts to a particular individual, and commented that this was often dependent upon circumstantial evidence.

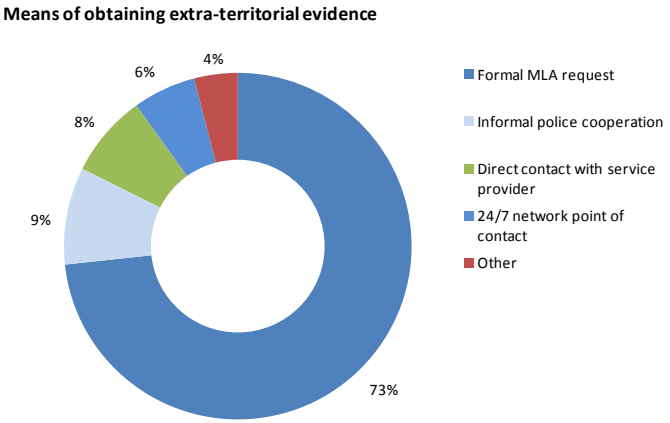
The challenges facing both law enforcement investigators and prosecutors mean that 'brought to justice' rates are low for cybercrime offenders. Suspects identified per police-recorded offence are comparable for child pornography offences to other sex offences. However, suspects per recorded offence for acts such as illegal access and computer-related fraud or forgery are only around 25 per 100 offences. Very few countries were able to provide data on persons prosecuted or convicted. Calculations for cybercrime offences in one country, however, show that the ratio of persons convicted to recorded offences, is significantly lower than for other 'conventional' crimes.

International cooperation

Countries responding to the study questionnaire report that between 30 and 70 per cent of cybercrime acts involve a transnational dimension, engaging issues of transnational investigations, sovereignty, jurisdiction, extraterritorial evidence, and a requirement for international cooperation. A transnational dimension to a cybercrime offence arises where an element or substantial effect of the offence is in another territory, or where part of the *modus operandi* of the offence is in another territory. International law provides for a number of bases of jurisdiction over such acts, including forms of territory-based jurisdiction and nationality-based jurisdiction. Some of these bases are also found in multilateral cybercrime instruments. While all countries in Europe consider that national laws provide a sufficient framework for the criminalization and prosecution of extraterritorial cybercrime acts, around one-third to over one-half of countries in other regions of the world report insufficient frameworks. In many countries, provisions reflect the idea that the 'whole' offence need not take place within the country in order to assert territorial jurisdiction. Territorial linkages can be made with reference

to elements or effects of the act, or the location of computer systems or data utilized for the offence. Where they arise, jurisdictional conflicts are typically resolved through formal and informal consultations between countries. Country responses do not reveal, at present, any need for additional forms of jurisdiction over a putative 'cyberspace' dimension. Rather, forms of territoriality-based and nationality-based jurisdiction are almost always able to ensure a sufficient connection between cybercrime acts and at least one State.

Forms of international cooperation include extradition, mutual legal assistance, mutual recognition of foreign judgments, and informal police-to-police cooperation. Due to the volatile nature of electronic evidence, international cooperation in criminal matters in the area of cybercrime requires timely responses and the ability to request specialized investigative actions, such as preservation of computer data. Use of traditional forms of cooperation predominates for obtaining extra-territorial evidence in cybercrime cases, with over 70 per cent of countries reporting using formal mutual legal assistance requests for this purpose. Within such formal cooperation, almost 60 per cent of requests use bilateral instruments as the legal basis. Multilateral instruments are used in 20 per cent of cases. Response times for formal mechanisms were reported to be of the order of months, for both extradition and mutual legal assistance requests, a timescale which presents challenges to the collection of volatile electronic evidence. Sixty per cent of countries in Africa, the Americas and Europe, and 20 per cent in Asia and Oceania, report channels for urgent requests. However, the impact of these on response times is unclear. Modes of informal cooperation are possible for around two-thirds of reporting countries, although few countries have a policy for the use of such mechanisms. Initiatives for informal cooperation and for facilitating formal cooperation, such as 24/7 networks, offer important potential for faster response times. They are, however, under-utilized, handling around three per cent of the total number of cybercrime cases encountered by law enforcement for the group of reporting countries.



Source: Study cybercrime questionnaire. Q105. (n=56, r=221)

Formal and informal modes of cooperation are designed to manage the process of State consent for the conduct of foreign law enforcement investigations that affect a State's sovereignty. Increasingly, however, investigators, knowingly or unknowingly, access extra-territorial data during evidence gathering, without the consent of the State where the data is physically situated. This situation arises, in particular, due to cloud computing technologies which involve data storage at multiple data centres in different geographic locations. Data 'location', whilst technically knowable, is becoming increasingly artificial, to the extent that even traditional mutual legal assistance requests will often be addressed to the country that is the seat of the service provider, rather than the country where the data centre is physically located. Direct foreign law enforcement access to extraterritorial data could occur when investigators make use of an existing live connection from a suspect's device, or where investigators use lawfully obtained data access credentials. Law enforcement investigators may,

on occasion, obtain data from extra-territorial service providers through an informal direct request, although service providers usually require due legal process. Relevant existing provisions on 'trans-border' access found in the Council of Europe Cybercrime Convention and the League of Arab States Convention on Information Technology Offences do not adequately cover such situations, due to a focus on the 'consent' of the person having lawful authority to disclose the data, and presumed knowledge of the location of the data at the time of access or receipt.

The current international cooperation picture risks the emergence of country clusters that have the necessary powers and procedures to cooperate amongst themselves, but are restricted, for all other countries, to 'traditional' modes of international cooperation that take no account of the specificities of electronic evidence and the global nature of cybercrime. This is particularly the case for cooperation in investigative actions. A lack of common approach, including within current multilateral cybercrime instruments, means that requests for actions, such as expedited preservation of data outside of those countries with international obligations to ensure such a facility and to make it available upon request, may not be easily fulfilled. The inclusion of this power in the draft African Union Cybersecurity Convention may go some way towards closing this lacuna. Globally, divergences in the scope of cooperation provisions in multilateral and bilateral instruments, a lack of response time obligation, a lack of agreement on permissible direct access to extraterritorial data, multiple informal law enforcement networks, and variance in cooperation safeguards, represent significant challenges to effective international cooperation regarding electronic evidence in criminal matters.

Cybercrime prevention

Crime prevention comprises strategies and measures that seek to reduce the risk of crimes occurring, and mitigate potential harmful effects on individuals and society. Almost 40 per cent of responding countries report the existence of national law or policy on cybercrime prevention. Initiatives are under preparation in a further 20 per cent of countries. Countries highlight that good practices on cybercrime prevention include the promulgation of legislation, effective leadership, development of criminal justice and law enforcement capacity, education and awareness, the development of a strong knowledge base, and cooperation across government, communities, the private sector and internationally. More than one half of countries report the existence of cybercrime strategies. In many cases, cybercrime strategies are closely integrated in cybersecurity strategies. Around 70 per cent of all countries reported national strategies included components on awareness raising, international cooperation, and law enforcement capacity. For the purposes of coordination, law enforcement and prosecution agencies are most frequently reported as lead cybercrime institutions.

Surveys, including in developing countries, demonstrate that most individual internet users now take basic security precautions. The continued importance of public awareness-raising campaigns, including those covering emerging threats, and those targeted at specific audiences, such as children, was highlighted by responding Governments, private sector entities, and academic institutions. User education is most effective when combined with systems that help users to achieve their goals in a secure manner. If user cost is higher than direct user benefit, individuals have little incentive to follow security measures. Private sector entities also report that user and employee awareness must be integrated into a holistic approach to security. Foundational principles and good practice referred to include accountability for acting on awareness, risk management policies and practices, board-level leadership, and staff training. Two-thirds of private sector respondents had conducted a

cybercrime risk assessment, and most reported use of cybersecurity technology such as firewalls, digital evidence preservation, content identification, intrusion detection, and system supervision and monitoring. Concern was expressed, however, that small and medium-sized companies either do not take sufficient steps to protect systems, or incorrectly perceive that they will not be a target.

Regulatory frameworks have an important role to play in cybercrime prevention, both with respect to the private sector in general and service providers in particular. Nearly half of countries have passed data protection laws, which specify requirements for the protection and use of personal data. Some of these regimes include specific requirements for internet service providers and other electronic communications providers. While data protection laws require personal data to be deleted when no longer required, some countries have made exceptions for the purposes of criminal investigations, requiring internet service providers to store specific types of data for a period of time. Many developed countries also have rules requiring organizations to notify individuals and regulators of data breaches. Internet service providers typically have limited liability as 'mere conduits' of data. Modification of transmitted content increases liability, as does actual or constructive knowledge of an illegal activity. Expeditious action after notification, on the other hand, reduces liability. While technical possibilities exist for filtering of internet content by service providers, restrictions on internet access are subject to foreseeability and proportionality requirements under international human rights law protecting rights to seek, receive and impart information.

Public-private partnerships are central to cybercrime prevention. Over half of all countries report the existence of partnerships. These are created in equal numbers by informal agreement and by legal basis. Private sector entities are most often involved in partnerships, followed by academic institutions, and international and regional organizations. Partnerships are mostly used for facilitating the exchange of information on threats and trends, but also for prevention activities, and action in specific cases. Within the context of some public-private partnerships, private sector entities have taken proactive approaches to investigating and taking legal action against cybercrime operations. Such actions complement those of law enforcement and can help mitigate damage to victims. Academic institutions play a variety of roles in preventing cybercrime, including through delivery of education and training to professionals, law and policy development, and work on technical standards and solution development. Universities house and facilitate cybercrime experts, some computer emergency response teams (CERTs), and specialized research centres.

Page left intentionally blank

CHAPTER ONE: CONNECTIVITY AND CYBERCRIME

This Chapter examines the effect of the global connectivity revolution on cybercrime and identifies cybercrime as a growing contemporary challenge driven by a range of underlying socio-economic factors. It considers definitions of cybercrime and finds that while certain definitions are required for 'core' cybercrime acts, the aggregate concept is not well suited as a legal term of art.

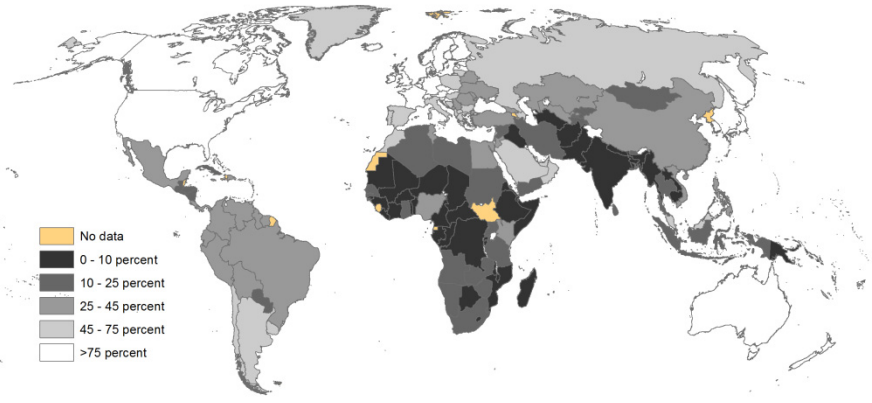
1.1 The global connectivity revolution

Key results:

- In 2011, more than one third of the world's total population had access to the internet
- Over 60 per cent of all internet users are in developing countries, with 45 per cent of all internet users below the age of 25 years
- It is estimated that mobile broadband subscriptions will approach 70 per cent of the world's total population by 2017
- The number of networked devices (the 'internet of things') are estimated to outnumber people by six to one, transforming current conceptions of the internet
- In the future hyper-connected society, it is hard to imagine a 'computer crime', and perhaps any crime, that does not involve electronic evidence linked with internet protocol (IP) connectivity

In 2011, at least 2.3 billion people – equivalent to more than one third of the world's total population – had access to the internet. Developed countries enjoy higher levels of internet access (70 per cent) than developing countries (24 per cent). However, the absolute number of internet users in developing countries already far outnumbers that in developed countries. Some 62 per cent of all internet users were in developing countries in 2011.

Figure 1.1: Percentage of internet users (2011)



Source: World Telecommunication/ICT Indicators 2012

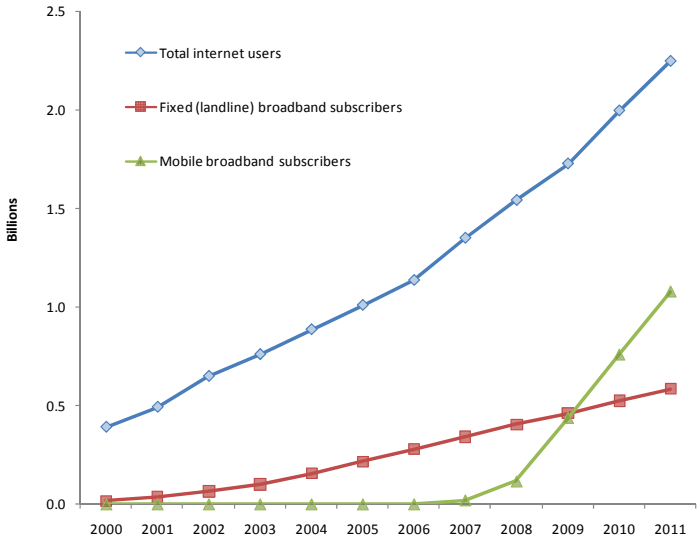
In both developed and developing countries, more younger people are online than older people. Some 45 per cent of the world's internet users are below the age of 25

years[1] – a demographic that also broadly corresponds with an age group often at special risk of criminal offending.[2]

The growth of mobile internet access

Almost 1.2 billion mobile broadband subscriptions exist globally. This is twice as many as fixed-line broadband subscriptions, and corresponds to around 16 per cent of the global population.[3] In 2009, the volume of global mobile data traffic overtook the volume of mobile voice traffic. Global mobile data traffic in 2011 was some four times greater than mobile voice traffic.[4]

Figure 1.2: Global internet connectivity 2000 - 2011



Source: ITU World Telecommunication ICT Indicators 2012

Africa and the Arab states show especially high ratios of mobile broadband to fixed broadband, reflecting the launch of high-speed 3G+ mobile networks and services in those regions, coupled with the growth in handheld devices, including smartphones and tablet computers. By 2017, GSM/EDGE[5] mobile technology is expected to cover more than 90 per cent of the world's population, with 85 per cent of the population accessing WCDMA/HSPA[6] mobile technology, at speeds of up to 2Mb per second. Forecasts suggest that the number of mobile broadband subscriptions will reach five billion by the year 2017. In 2011, the number of networked *devices* – the so-called 'internet of things' – overtook the total global population. By 2020, the number of connected devices may outnumber connected people by six to one, potentially transforming current conceptions of the internet.[7] Whereas connected persons currently have at least one or both of two devices connected to the internet (typically a computer and smartphone), this could rise to seven devices by 2015.[8] In the 'internet of things,' objects such as household appliances, vehicles, power and water meters, medicines or even personal belongings such as clothes, will be capable of being assigned an IP address, and of identifying themselves and communicating using technology such as RFID and NFC.[9]

---

1 International Telecommunication Union, 2012. *Measuring the Information Society, and World Telecommunication/ICT Indicators Database.* See also Moore, R., Guntupalli, N.T., and Lee, T., 2010. Parental regulation and online activities: Examining factors that influence a youth's potential to become a victim of online harassment. *International Journal of Cyber Criminology,* 4(1&2):685–698.

2 European Commission, 2012. *Special Eurobarometer 390: Cyber Security Report.* See also Fawn, T. and Paternoster, R., 2011. Cybercrime Victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, 5(1):773-793, 782.

3 International Telecommunication Union, 2012. *Measuring the Information Society, and World Telecommunication/ICT Indicators Database.*

4 Ericsson, 2012. *Traffic and Market Report.*

5 Global System for Mobile Communications/Enhanced Data rates for GSM Evolution, or EGPRS.

6 Wideband Code Division Multiple Access/High Speed Packet Access.

7 International Telecommunication Union, 2012. *The State of Broadband 2012: Achieving Digital Inclusion For All.*

8 European Commission, 2012. *Digital Agenda: Commission consults on rules for wirelessly connected devices – the 'Internet of Things.'* Available at: http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=IoTGovernance

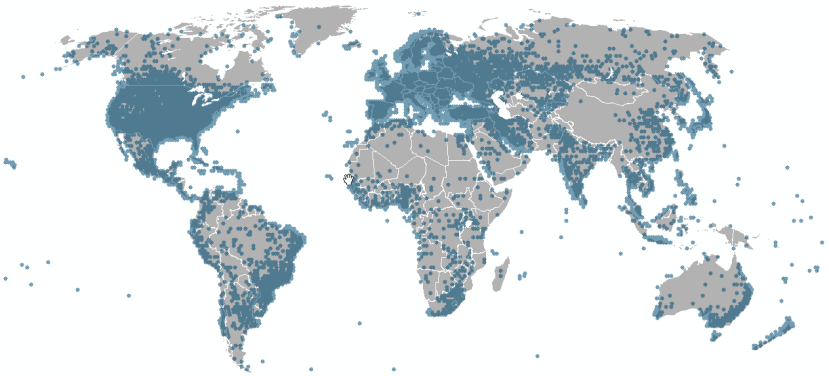
9 Radio-frequency identification and Near field communication.

The persisting digital divide

Disparities in internet access are vividly illustrated by mapping the geo-location of global IP addresses. This provides a reasonable approximation of the geographic reach of the internet. While IP address density largely follows global population density, a number of populated locations in developing countries show sparse internet connection availability. Gaps in Southern and Eastern Asia, Central America, and Africa, in particular, exemplify the present digital divide. As of mid-2012, some 341 million people in sub-Saharan Africa live beyond a 50km range of a terrestrial fibre-optic network – a number greater than the population of the United States of America.[10]

As noted by the Broadband Commission for Digital Development established by ITU and UNESCO, regions not connected to the internet miss its unprecedented potential for economic opportunity and social welfare. The World Bank estimates that a 10 per cent increase in broadband penetration would yield, on average, a 1.38 per cent increase in GDP growth in low and middle income countries.[11] Mobile broadband has been found to have a higher impact on GDP growth than fixed broadband through the reduction of inefficiencies.[12] Beyond economic growth, the internet enables access to vital services for the most remote, including education, healthcare, and e-governance.

Figure 1.3: IP geolocation (2012)



Source: UNODC elaboration of MaxMind GeoCityLite.

The role of the private sector

A significant proportion of internet infrastructure is owned and operated by the private sector. Internet access requires a 'passive' infrastructure layer of trenches, ducts, optical fibre, mobile base stations, and satellite hardware. It also requires an 'active' infrastructure layer of electronic equipment, and a 'service' layer of content services and applications.[13] Large global ISPs, such as AT&T, NTT Communications, Sprint, Telefonica, and Verizon, own or lease high capacity inter- and intra-continental fibre optic transport (the internet *backbone*) as well as other core internet infrastructure, such as switches and routers. ISP networks are connected both bilaterally, and at concentrated points (known as *internet exchange points*, or IXPs). Major networks negotiate *peering agreements* among themselves, whereby each agrees to carry the other's traffic – this allows them to provide fast global connections to their clients. They also carry paid-for data for non-peering networks. Mobile telephone operators and local ISPs own or manage the network of radio cells and local cables that bring the internet the 'last kilometre' from server to handheld and desktop devices. Annex Four to this Study contains further details about internet infrastructure.

---

10 Commonwealth Telecommunications Organisation, 2012. *The Socio-Economic Impact of Broadband in sub-Saharan Africa: The Satellite Advantage.*

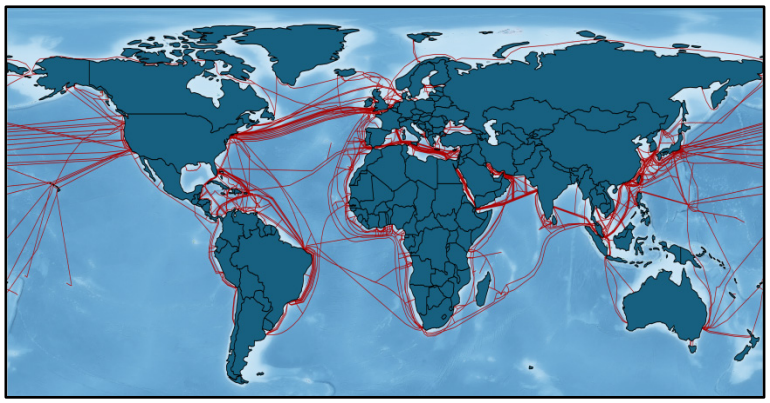
11 World Bank, 2009. *Information and Communications for Development: Extending Reach and Increasing Impact.*

12 World Bank, 2012. *Information and Communications for Development: Maximizing Mobile.*

13 International Telecommunication Union, 2012. *The State of Broadband 2012: Achieving Digital Inclusion For All.*

As global operators seek to build broad business bases, and to maximize efficiency and returns on infrastructure investment, recent years have seen a convergence of traditionally distinct information technologies, communication technologies, and web services.[14] Telecommunications networks are evolving into all-IP data networks, with standardized products and simpler interconnectivity. Increased cloud storage and computing will enable the same services and user content to be delivered to any user device, whether a mobile phone, desktop or tablet computer.

Figure 1.4: Global submarine cables



Source: UNODC elaboration of data from http://www.cablemap.info/

IP technology generally reduces the cost of commercial network operations. However, the cost of international bandwidth can still vary enormously, depending upon the elasticities of supply and demand. Until, for example, the ACE (Africa Coast to Europe) submarine cable becomes fully operational, countries in Western Africa remain burdened with some of the highest internet connectivity costs in the world, due to exclusive reliance on commercial satellite bandwidth.[15]

As an infrastructure, the internet's growth can be compared to the development of roads, railways, and electricity, which are dependent on private sector investment, construction and maintenance, but regulated and incentivized by national governments. At the same time, the internet is often regarded as more private-sector led. Working with the private sector, governments can offer public sector policy leadership and facilitate growth of the internet through direct investment in infrastructure and services, by putting in place policies that promote competition and remove investment barriers, and by providing incentives to enterprises that deploy internet services.[16]

1.2 Contemporary cybercrime

Key results:

- Computer-related crime is a long-established phenomenon, but the growth of global connectivity is inseparably tied to the development of contemporary cybercrime
- Today's cybercrime activities focus on utilizing *globalized* information communication technology for committing criminal acts with *transnational* reach
- Some cybercrime is committed using stand-alone or closed computer systems, although much less frequently

In addition to its socio-economic benefits, there is no doubt that computer technology and

14 World Economic Forum, 2012. *The Global Information Technology Report 2012: Living in a Hyperconnected World.*
15 Commonwealth Telecommunications Organisation, 2012. *The Socio-Economic Impact of Broadband in sub-Saharan Africa: The Satellite Advantage.*
16 World Economic Forum, 2012. *The Global Information Technology Report 2012: Living in a Hyperconnected World.*

the internet – just as with other means enhancing capabilities of human interaction – can be used for criminal activity. While computer-related crime, or computer crime, is a comparatively long-established phenomenon, the growth of global connectivity is inherent to contemporary cybercrime.

Computer-related acts including physical damage to computer systems and stored data;[17] unauthorized use of computer systems and the manipulation of electronic data;[18] computer-related fraud;[19] and software piracy[20] have been recognized as criminal offences since the 1960s.

In 1994, the United Nations Manual on the Prevention and Control of Computer Related Crime noted that fraud by computer manipulation; computer forgery; damage to or modifications of computer data or programs; unauthorized access to computer systems and service; and unauthorized reproduction of legally protected computer programs were common types of computer crime.[21]

While such acts were often considered local crimes concerning stand-alone or closed systems, the *international* dimension of computer crime and related criminal legislation was recognized as early as 1979. A presentation on computer fraud at the Third INTERPOL Symposium on International Fraud, held from 11 to 13 December 1979, emphasized that '*the nature of computer crime is international, because of the steadily increasing communications by telephones, satellites etc., between the different countries.*'[22]

The core concept at the heart of today's cybercrime remains exactly that – the idea that converging *globalized* information communication technology may be used for committing criminal acts, with *transnational* reach.

These acts may include all of the computer-related crimes listed above, in addition to many others, such as those related to computer or internet content,[23] or computer-related acts for personal or financial gain.[24] As set out in this Chapter, this Study does not 'define' contemporary cybercrime as such. It rather describes it as a list of acts which constitute cybercrime. Nonetheless, it is clear that the focus is on the misuse of ICT from a *global perspective*. More than half of responding countries, for example, reported that between 50 and 100 per cent of cybercrime acts encountered by the police involve a *transnational* element.[25] Respondents referred to cybercrime as a *'global phenomenon'* and noted that *'online communication invariably involves international or transnational dimensions.*'[26]

Placing the focus on global connectivity does not exclude crimes involving stand-alone or closed computer systems from the scope of cybercrime.[27] Interestingly, while law enforcement officials in developed countries typically identified a high proportion of cybercrime with a transnational element, those in developing countries tended to identify a much lower proportion –

---

17 Regarding related challenges, see Slivka, R.T., and Darrow, J.W., 1975. Methods and Problems in Computer Security. *Rutgers Journal of Computers and Law,* 5:217.

18 United States Congress, 1977. *Bill S.1766, The Federal Computer Systems Protection Act,* 95th Congress, 1st Session., 123 Cong. Rec. 20, 953 (1977).

19 Glyn, E.A., 1983. Computer Abuse: The Emerging Crime and the Need for Legislation. *Fordham Urban Law Journal*, 12(1):73-101.

20 Schmidt, W.E., 1981. Legal Proprietary Interests in Computer Programs: The American Experience. *Jurimetrics Journal,* 21:345.

21 United Nations, 1994. *UN Manual on the Prevention and Control of Computer Related Crime.*

22 INTERPOL, 1979. *Third INTERPOL Symposium on International Fraud,* Paris 11-13 December 1979.

23 Including computer-related acts involving racism or xenophobia, or computer-related production, distribution, or possession of child pornography.

24 Including computer-related identity offences, and computer-related copyright and trademark offences.

25 Study cybercrime questionnaire. Q83.

26 *Ibid.*

27 Some approaches hold that cybercrime is narrower than 'computer-related' crime, insofar as cybercrime is said to require the involvement of a computer *network* – thereby excluding crimes committed using a stand-alone computer system. While focusing on the feature of connectivity, this Study does not strictly exclude stand-alone or closed computer systems from the scope of cybercrime. Thus, the term 'cybercrime' is used to describe a range of offences including traditional computer crimes, as well as network crimes.

fewer than 10 per cent in some cases.[28] On the one hand, this may indicate that cybercrime perpetrators in developing countries focus more on domestic victims and (possibly, stand-alone) computer systems. On the other, it may also be the case that, due to capacity challenges, law enforcement in developing countries less frequently identify, or engage with, foreign service providers or potential victims linked with national cases.

Nonetheless, the reality of global connectivity must be considered as a central element to contemporary cybercrime and, in particular, the cybercrime of tomorrow. As cyberspace and IP traffic grows,[29] as traffic from wireless devices exceeds traffic from wired devices, and as more internet traffic originates from non-PC devices, it may become hard to imagine a 'computer' crime without the fact of IP connectivity. The particularly personal nature of mobile devices, and the emergence of IP-connected household or personal effects, means that electronic data and transmissions could even be generated by, or become integral to, almost every human action – whether legal or illegal.

1.3 Cybercrime as a growing challenge

Key results:

- Because of the difficulties arising when trying to define and identify cybercrime, cross-nationally comparative statistics on cybercrime are much rarer than for other crime types
- At the global level, law enforcement respondents to the Study perceive increasing levels of cybercrime, as both individual offenders and organized criminal groups exploit new opportunities, driven by profit and personal gain
- Cybercrime is advancing in the focus of the public due to increased media reporting of cybercrime cases, cybersecurity issues and other cyber-related news
- Criminological theories and socio-economic approaches offer possible explanations for the recent growth in cybercrime activities
- In many countries across all regions, the explosion in global connectivity has come at a time of economic and demographic transformations, with rising income disparities, tightened private sector spending, and reduced financial liquidity

The increasing ubiquity of global connectivity presents a serious risk that rates of cybercrime will increase. While reliable statistics are hard to obtain, many country respondents to the Study questionnaire indicated that cybercrime is a growing challenge – a plausible viewpoint given underlying criminological and socio-economic factors. One responding country from Europe, for example, noted that: '*Relying upon research and statistics provided mostly by the private sector or the academia, it is commonly agreed upon that cybercrime acts are increasing dramatically, with a limited powers to control it.*'[30] In the 2010 Salvador Declaration on Comprehensive Strategies for Global Challenges, annexed to General Assembly resolution 65/230, it was noted that the '*development of information and communications*

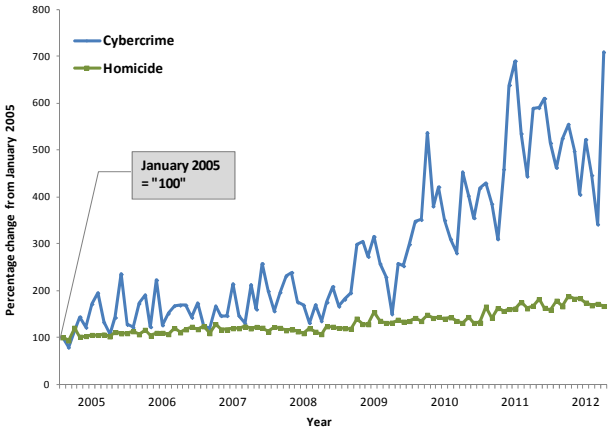
[28] Study cybercrime questionnaire. Q83.
[29] In 2016 the gigabyte equivalent of all movies ever made will cross global IP networks every 3 minutes. Cisco, 2012. *Cisco Visual Networking Index, 2011-2016*.
[30] Study cybercrime questionnaire. Q84.

technologies and the increasing use of the Internet create new opportunities for offenders and facilitate the growth of crime.'[31]

Due to significant challenges in the measurement of cybercrime, cross-nationally comparative statistics on cybercrime are much rarer than for other crime types.[32] Annex Two to this Study examines current methodological approaches to measuring cybercrime, and presents some of the few available statistics.

In the past five years in particular, the issue of cybercrime has come prominently to the forefront of public discussion, including in developing countries. A search of global news wires for the terms 'cybercrime' and 'homicide', in the six official United Nations languages, reveals a significant relative growth in the frequency of global news references to cybercrime, as compared with references to homicide. Between the years 2005 and 2012, references to cybercrime have increased by up to 600 per cent, compared with around 80 per cent in the case of references to homicide.[33] Such measurements are not directly related to underlying cybercrime acts. Nonetheless, they can reflect general global 'activity' concerning cybercrime – including media reporting on government initiatives and counter measures.

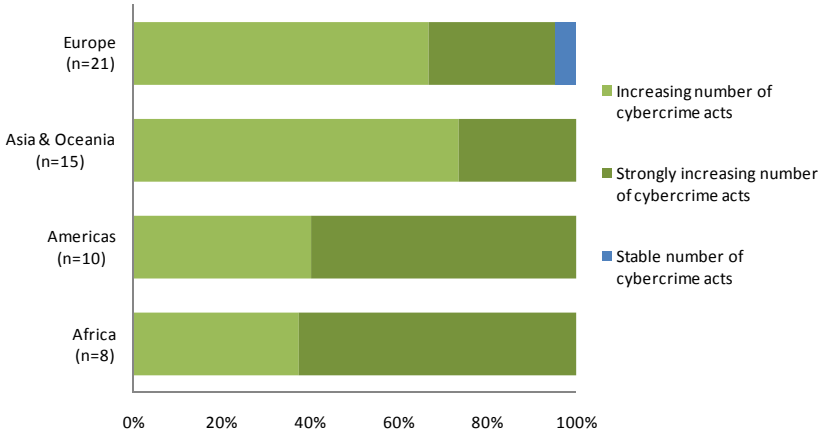
Figure 1.5: Relative frequency of global news reports 2005-2012



Source: UNODC calculations from Dow Jones Factiva.

The views of law enforcement officials also reflect a consensus that levels of cybercrime are increasing. When asked about cybercrime trends observed in their own country over the past five years, all law enforcement officials in 18 countries in Africa, and the Americas responded that cybercrime was either increasing or strongly increasing.[34] Law

Figure 1.6 : Cybercrime trends observed by law enforcement 2007-2011



Source: Study cybercrime questionnaire. Q84 (n=54).

31 *Salvador Declaration on Comprehensive Strategies for Global Challenges*, annex to United Nations General Assembly Resolution A/Res/65/230 on the *Twelfth United Nations Congress on Crime Prevention and Criminal Justice*, 1 April 2011, para.39.

32 United Nations Statistical Commission, 2012. *National Institute of Statistics and Geography of Mexico Report on Crime Statistics*. Note by the Secretary General E/CN.3/2012/3, 6 December 2011.

33 UNODC calculations from Dow Jones Factiva.

34 Study cybercrime questionnaire. Q84. Due to variable preparation and release times for official statistics, this may refer to the time

enforcement officials in Europe and Asia and Oceania tended to view cybercrime as increasing, rather than strongly increasing; and a small number of countries in Europe were of the view that the phenomenon was stable.[35]

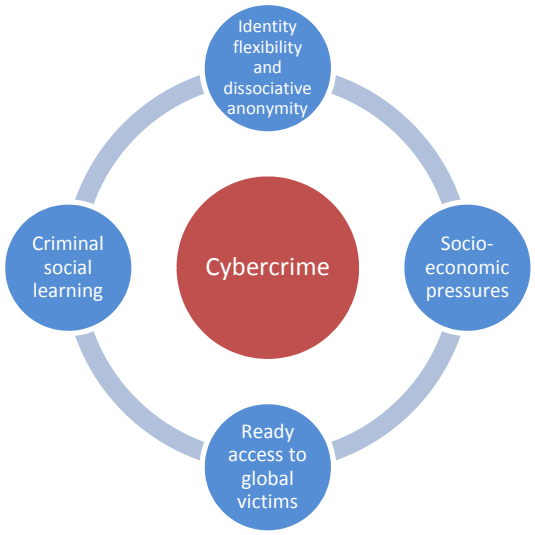
Law enforcement officials referred to a range of cybercrime acts as increasing, including computer-related fraud and identity theft; computer-related production, distribution or possession of child pornography; phishing attempts; and illegal access to computer systems, including hacking. Increasing levels of cybercrime are attributed by law enforcement officials in part to a growing capability in the area of anonymity techniques when using ICT, as well as the growing commercialization of computer misuse tools. Chapter Two (The global picture) further analyses information provided by states and the private sector on trends in and threats from specific cybercrime acts.

Underlying factors: Criminological and socio-economic approaches

From a criminological perspective, the suggestion that ICT and the increasing use of the internet create new opportunities for offenders and facilitates the growth of crime is highly plausible. While a number of different criminological theories are applicable, the fact that cybercrime represents *'a new and distinctive format of crime,'*[36] creates challenges to predicting developments, and to its prevention, by the application of general crime theories.[37]

One key proposition is that the emergence of 'cyberspace' creates new phenomena that are notably distinct from the (mere) existence of computer systems themselves, and the direct opportunities for crime that computers present. Within cyberspace, persons may show differences between their conforming (legal) and non-conforming (illegal) behaviour as compared with their behaviour in the physical world. Persons may, for example, commit crimes in cyberspace that they would not otherwise commit in physical space due to their status and position. In addition, identity flexibility, dissociative anonymity and a lack of deterrence factors may provide incentives for criminal behaviour in cyberspace.[38]

Figure 1.7: Possible underlying factors linked to increases in cybercrime



Routine activity theory (RAT)[39] may also provide insight into underlying drivers of cybercrime. RAT proposes that crime risk increases upon the convergence of: (1) a motivated

---

period of 2007 to 2011 or 2006 to 2010 ('the last five years').

35 *Ibid.*

36 Yar, M., 2005. The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology,* 2(4):407-427.

37 Koops, B.J., 2010. The Internet and its Opportunities for Crime. *In:* Herzog-Evans, M., (ed.) *Transnational Criminology Manual.* Nijmegen, Netherlands: WLP, pp.735-754.

38 Jaishankar. K., 2011. Expanding Cyber Criminology with an Avant-Garde Anthology. *In:* Jaishankar, K., (ed.) *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour.* Boca Raton, FL: CRC Press, Taylor & Francis Group.

39 Kigerl, A., 2012. Routine Activity Theory and the Determinants of High Cybercrime Countries. *Social Science Computer Review,* 30(4):470-486, 470.

offender, (ii) a suitable target, and (iii) the absence of a capable guardian.[40] In the case of cybercrime, large numbers of suitable targets may emerge through increasing time spent online, and the use of online services such as banking, shopping and file sharing – making users prone to phishing attacks or fraud.[41] The emergence of online social networks, including Twitter and Facebook, also provides a ready supply of millions of potential scam or fraud victims. Where users have not restricted communication settings to enable only interaction with their private network of 'friends', such networks can enable accessibility of a large number of potential victims all at once. Persons also tend to organize their social networking profiles according to their interests and location, which enables criminals to target victims with specific modes of behaviour or backgrounds. Such 'guardian' measures that do exist, such as anti-virus programmes and a (comparatively small) risk of law enforcement action, can be insufficient to deter a perpetrator motivated by the lure of significant profit.

Research also highlights that the general theory of crime concerning reduced self-control and a preparedness to assume risk for short-term gains, may apply to acts that can be facilitated or enhanced by electronic communications and the internet. In addition, individuals exposed online to cyber criminal models and peers may themselves be more likely to engage in cybercrime.[42] This 'social-learning' theory may have particular application when it comes to cybercrime, as offenders often need to learn specific computer techniques and procedures.[43] Social learning theory and the general theory of crime interact, in that persons with reduced self-control may actively seek out similar others and coalesce in virtual environments in the same way as in the real world. In cyberspace this process can occur in a significantly reduced timeframe, and with much broader geographic reach.

Online connectivity and peer-learning is likely central to the engagement of organized criminal groups in cyber criminality. Online 'carding' or 'carder' forums for the exchange of stolen credit card details are one such example. 'Carder' forums have often commenced with a 'swarm' structure with no obvious chain of command as cyber perpetrators seek out one another and 'meet' online for exchange of knowledge and the provision of criminal services. Forums later evolve into more controlled 'hub'-like operations with higher degrees of criminal organization.[44] The use of social networking sites can also enable forms of social 'outreach' and connectivity between individuals and criminal groups.[45]

Another underlying development that may contribute to driving cybercrime levels is the emergence of global connectivity in the context of world economic and demographic transformations. By 2050, the world will experience a near doubling of the urban population to 6.2 billion – 70 per cent of the projected world population of 8.9 billion.[46] The World Economic Forum Global Risks Report 2012 cites severe income disparity and chronic fiscal imbalances as two of the

---

40 *Ibid.*

41 For an overview and further references, see *ibid.* p.473; Hutchings, A., Hennessey, H., 2009. Routine activity theory and phishing victimization: Who got caught in the 'net'? *Current Issues in Criminal Justice,* 20(3):433-451; Pratt, T.C., Holtfreter, K., Reisig, M.D., 2010. Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, 47(3):267-296.

42 Holt, T.J., Burruss, G.W., Bossler, A.M., 2010. Social Learning and Cyber Deviance: Examining the Importance of a Full Social Learning Model in the Virtual World. *Journal of Crime and Justice*, 33(2):31-61.

43 Skinner, W.F., Fream, A.M., 1997. A Social Learning Theory Analysis of Computer Crime among College Students. *Journal of Research in Crime and Delinquency*, 34(4):495-518.

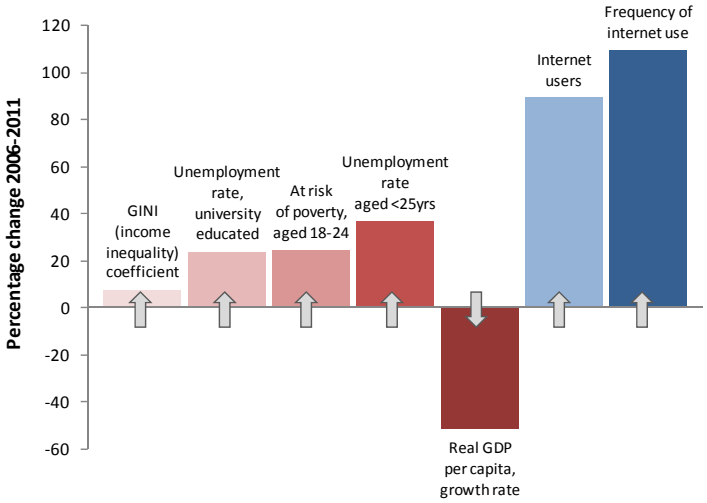
44 BAE Systems Detica and John Grieve Centre for Policing and Security, London Metropolitan University, 2012. *Organised Crime in the Digital Age.*

45 A number of Twitter feeds, for example, either purport to represent individuals associated with hacking groups such as Anonymous or Lulzsec, or the organizations themselves.

46 World Economic Forum, 2011. *Outlook on the Global Agenda 2011.*

top five global risks in the year 2012.[47] Gallup polling data from 2011 reveal that, globally, people perceive their living standards to be falling – a discontent exacerbated by stark income disparities.[48] UNODC research shows that economic factors play an important role in the evolution of crime trends. Out of a total of 15 countries examined, statistical modelling suggested some overall association between economic changes and three conventional crime types in 12 countries.[49]

Figure 1.8: Socio-economic changes and frequency of internet use in one Eastern European country 2006-2011



Source: Eurostat and ITU World Telecommunication ICT Indicators 2012

Socio-economic factors may also play an important role in increases in cybercrime. Pressure on private sector enterprises to cut spending and to reduce staffing levels can lead, for example, to reductions in security, and to opportunities for exploitation of ICT weaknesses.[50] As firms are forced to hire in outside or temporary contractors, or employees become disgruntled by lower wages and fear of job loss, the risk both of lone criminal actions and influence by organized criminal groups over company 'insiders' may increase.[51] Some cybersecurity companies have expressed concern that former employees who have been made redundant pose one a possible threat during periods of economic downturn.[52] Increasingly large numbers of unemployed or underemployed graduate students with computing skills have also been reported to offer potential new resources for organized crime.[53]

The role of socio-economic factors in cybercrime is not limited to the developed world. Rather, it is equally applicable in the developing country context. In one country in Western Africa, for example, studies on the socio-demographic characteristics of *yahooboys*[54] show that many are university students who view online fraud as a means of economic sustenance.[55] Unemployment, in particular, is identified as a crucial factor luring youths to *yahooboyism*.[56] Studies in another country in Africa similarly highlight that '*Sakawa*' boys engaged in internet fraud frequently justify their

47 World Economic Forum, 2012. *Global Risk Report 2012.*
48 *Ibid*, citing Credit Suisse Research Institute, 2011. *Global Wealth Report 2011.*
49 UNODC, 2011. *Monitoring the Impact of Economic Crisis on Crime.*
50 BAE Systems Detica and John Grieve Centre for Policing and Security, London Metropolitan University, 2012. *Organised Crime in the Digital Age.*
51 *Ibid.*
52 McAfee, 2009. *Unsecured Economies: Protecting Vital Information.*
53 BAE Systems Detica and John Grieve Centre for Policing and Security, London Metropolitan University, 2012. *Organised Crime in the Digital Age.*
54 The sub-culture of '*yahooboys*' describes youths, especially those living in cities, who make use of the internet for acts of computer-related fraud, phishing and scamming. Adeniran, A.I., 2011. Café Culture and Heresy of Yahooboyism. *In:* Jaishankar, K., (ed.) *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour.* Boca Raton, FL: CRC Press, Taylor & Francis Group.
55 Adeniran, A.I., 2008. The Internet and Emergence of Yahooboys sub-Culture. *International Journal of Cyber Criminology*, 2 (2):368-381; and Aransiola, J.O., Asindemade, S.O., 2011. Understanding Cybercrime Perpetrators and the Strategies They Employ. *Cyberpsychology, Behaviour and Social Networking*, 14(12):759.
56 *Ibid.*

activities as being the only way that they can survive in the absence of employment.[57]

The contemporary growth of cybercrime is important due to its impact and threat on multiple levels. Asked about the threat of cybercrime, law enforcement officials referred to a range of impacts. These included the fact that some cybercrime acts, such as online fraud and identity-theft, represent a threat because they are very common, producing an aggregate impact from the volume of offending and cumulative effects. Chapter Two (The global picture) of this Study examines the extent of the financial impact of cybercrime on individuals and companies. Such acts may also generate resources for organized criminal groups that may be used to support further crimes. Other cybercrime acts, such as the creation of illegal computer-misuse tools, may be quite rare, but pose a significant threat because individual incidents may cause great harm. A third category includes offences which cause harm to individuals, such as the creation and online dissemination of child pornography.[58]

1.4 Describing cybercrime

Key results:

- 'Definitions' of cybercrime mostly depend upon the purpose of using the term
- A limited number of acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime
- Computer-related acts for personal or financial gain or harm, including forms of identity-related crime, and computer content-related acts do not lend themselves easily to efforts to arrive at legal definitions of the aggregate term
- Certain definitions are required for the core of cybercrime acts. However, a 'definition' of cybercrime is not as relevant for other purposes, such as defining the scope of specialized investigative and international cooperation powers, which are better focused on electronic evidence for any crime, rather than a broad, artificial 'cybercrime' construct

A comprehensive Study on cybercrime must be clear on the range of acts that are included in the term. The word 'cybercrime' itself is not amenable to a single definition, and is likely best considered as a *collection* of acts or conduct, rather than one single act. Nonetheless, the basic content of the term can be described – at least for the purposes of this Study – by a non-exhaustive list of acts that constitute cybercrime. These acts can, in turn, be organized into categories based on the material offence object and *modus operandi*.

The term 'cybercrime'

Numerous academic works have attempted to define 'cybercrime.'[59] National legislation, however, does not appear concerned with a strict definition of the word. Out of almost 200 items of national legislation cited by countries in response to the Study questionnaire, fewer than five per

---

57 Warner, J., 2011. Understanding Cybercrime: A View from Below. *International Journal of Cyber Criminology*, 5(1):736-749.

58 Study cybercrime questionnaire. Q81.

59 Among various others, International Telecommunication Union, 2011. *Understanding Cybercrime: A Guide for Developing Countries*; Explanatory Report to the Council of Europe Cybercrime Convention, ETS No. 185; Pocar, F., 2004. New challenges for international rules against cyber-crime. *European Journal on Criminal Policy and Research,* 10(1):27-37; Wall, D.S., 2007. *Cybercrime: The Transformation of Crime in the Information Age.* Cambridge: Polity Press.

cent used the word 'cybercrime' in the title or scope of legislative provisions.[60] Rather, legislation more commonly referred to *'computer crimes,'*[61] *'electronic communications,'*[62] *'information technologies,'*[63] or *'high-tech crime.'*[64] In practice, many of these pieces of legislation created criminal offences that are included in the concept of cybercrime, such as unauthorized access to a computer system, or interference with a computer system or data. Where national legislation did specifically use cybercrime in the title of an act or section (such as 'Cybercrime Act'), the definitional section of the legislation rarely included a definition for the word 'cybercrime.'[65] When the term 'cybercrime' *was* included as a legal definition, a common approach was to define it simply as *'the crimes referred to in this law.'*[66]

In a similar manner, very few international or regional legal instruments define cybercrime. Neither the Council of Europe Cybercrime Convention, the League of Arab States Convention, nor the Draft African Union Convention, for example, contain a definition of cybercrime for the purposes of the instrument. The Commonwealth of Independent States Agreement, without using the term 'cybercrime,'[67] defines an 'offence relating to computer information' as a '*criminal act of which the target is computer information.*'[68] Similarly, the Shanghai Cooperation Organization Agreement defines 'information offences' as '*the use of information resources and (or) the impact on them in the informational sphere for illegal purposes.*'[69]

The definitional approaches apparent from national, international and regional instruments inform the method adopted by this Study. The Study does not seek to 'define' cybercrime *per se*. Rather, it identifies a list, or 'basket', of acts which could constitute cybercrime. This has the advantage of placing the focus on careful description of the precise conduct to be criminalized. As such, the word 'cybercrime' itself may be better *not* considered as a legal term of art.[70] It is notable that this is equivalent to the approach adopted by international instruments such as the United Nations Convention against Corruption.[71] This instrument does not define 'corruption', but rather obliges States Parties to criminalize a specific set of conduct which can be more effectively described.[72] 'Cybercrime' is therefore best considered as a *collection* of acts or conduct.

Describing surrounding concepts

It is also instructive to examine descriptions of surrounding concepts, such as 'computer', 'computer system', 'data' and 'information.' Their meaning is inherent to understanding the objects and/or protected legal interests which cybercrime acts concern. A review of international and regional instruments shows two main approaches: (i) terminology based on 'computer' data or

---

60 Study cybercrime questionnaire. Q12.
61 See, for example, Malaysia, Computer Crimes Act 1997; Sri Lanka, Computer Crime Act 2007; Sudan, Computer Crimes Act 2007.
62 See, for example, Albania, Electronic Communications in the Republic of Albania, Law no. 9918 2008; France, Code des postes et des communications électroniques (version consolidée) 2012; Tonga, Communications Act 2000.
63 See, for example, India, The Information Technology Act 2000; Saudi Arabia, IT Criminal Act 2007; Bolivarian Republic of Venezuela, Ley Especial contra los Delitos Informáticos 2001; Vietnam, Law on Information Technology 2007.
64 See, for example, Serbia, Law on Organization and Competence of Government Authorities for Combating High-Tech Crime 2010.
65 See, for example, Botswana, Cybercrime and Computer Related Crimes Act 2007; Bulgaria, Chapter 9, Criminal Code SG No. 92/2002; Cambodia, Draft Cybercrime Law 2012; Jamaica, Cybercrimes Act 2010; Namibia, Computer Misuse and Cybercrime Act 2003; Senegal, Law No. 2008-11 on Cybercrime 2008.
66 See for example, Oman, Royal Decree No 12/2011 issuing the Cybercrime Law; Philippines, Cybercrime Prevention Act 2012.
67 The original agreement is in Russian language and uses the term 'преступление в сфере компьютерной информации', rather than the contemporary equivalent to 'cybercrime': 'киберпреступности.'
68 Commonwealth of Independent States Agreement, Art. 1(a).
69 Shanghai Cooperation Organization Agreement, Annex 1.
70 See also International Telecommunication Union, 2011. *Understanding Cybercrime: A guide for Developing Countries.*
71 United Nations. 2004. *Convention against Corruption.*
72 *Ibid.*, Arts. 15 et seq.

system; and (ii) terminology based on 'information' data or system.[73] Analysis of the elements of the definitions, however, suggests that the terms might be considered as largely interchangeable. The figure shows common elements from these definitions. While nomenclature varies, a number of core concepts are consistent.

Computer/information system

- Device [or interconnected devices] which [pursuant to a computer/information program] perform(s) [[automatic] processing of computer data/information] [logical/arithmetic/storage functions] [including computer data/information stored/processed/retrieved/transmitted by the computer/information system] [including any communications facility or equipment] [including the internet]

Computer/information program

- Instructions [in machine readable form] that [enable a computer/information system to [process computer data/information] [perform a function/operation]] [can be executed by a computer/information system]

Computer data/information

- Representation of facts/information/concepts [in a machine readable form] [suitable for processing by a computer/information program [or a computer/information system]] [including a computer/information program]

The core feature of legal descriptions of 'computer', 'computer system' or 'information system', for example, is that the device must be 'capable of processing computer data or information.'[74] Some approaches specify that the processing must be 'automatic,' or 'high speed,' or 'pursuant to a program.'[75] Some approaches extend the definition to devices that store or transmit and receive computer data or information.[76] Others include within the definition the computer data that is processed by the system.[77] Where the term 'computer system' or 'information system' excludes data stored in the system or in other storage devices, these are often handled separately in the substantive legal provisions of the instrument.[78] While some instruments define both 'computer' and 'computer system,' the latter normally includes the former, and the context of the use of both terms in the instrument suggests that no meaningful difference arises in practice.[79] Other instruments define both 'computer network' and 'computer system.'[80] Again, it is possible that the latter includes the former, and there does not appear to be a distinguishable difference in use within the instrument itself.

International and regional cybercrime legal instruments are predominantly 'technology-

---

73 The Council of Europe Cybercrime Convention and the Commonwealth Model Law make use of the terms 'computer system' and 'computer data.' The Draft African Union Convention uses 'computer system' and 'computerized data.' The EU Decision on Attacks against Information Systems makes use of 'information system' and 'computer data.' The League of Arab States Convention makes use of 'information system' and 'data', and the Commonwealth of Independent States Agreement uses 'computer information.'

74 See, for example, Council of Europe Cybercrime Convention, Art. 1.

75 See, for example, COMESA Draft Model Bill, Art.1 and ITU/CARICOM/CTU Model Legislative Texts, Art. 3.

76 Draft African Union Convention, Part III, Section 1, Art. III-1(6).

77 EU Decision on Attacks against Information Systems, Art. 1(a).

78 See, for example, Council of Europe Cybercrime Convention, Art. 19, procedural power for competent authorities to search or similarly access (a) a computer system or part of it and computer data stored therein; and (b) a computer-data storage medium in which computer data may be stored.

79 COMESA Draft Model Bill, Part 1, Art. 1(b) and (e).

80 League of Arab States Convention, Art. 2(5) and (6).

neutral' in their text. They do not specifically list devices that might be considered as computer systems or information systems. In most contexts, this approach is considered good practice, insofar as it mitigates the risk of new technologies falling outside of legal provisions and the need for continuous updating of legislation.[81] Based on the core concept of processing computer data or information, it is likely that provisions typically apply to devices such as mainframe and computer servers, desktop personal computers, laptop computers, smartphones, tablet devices, and on-board computers in transport and machinery, as well as multimedia devices such as printers, MP3 players, digital cameras, and gaming machines.[82] Under the concept of 'processing computer data or information,' it is strongly arguable that any device, such as a wireless or fixed router, that connects to the internet is also included. Storage devices such as hard disk drives, USB memory sticks or flash cards may or may not strictly be part of the 'computer system' or 'information system.' But, where they are not, they can still be relevant objects through separate legal provisions.

Only one international or regional instrument attempts a 'lower technology' limit on the description of a computer system – stating that the term does not include an *'automated typewriter or typesetter, a portable hand held calculator, or other similar device.'*[83] As the world moves towards an 'internet of things' and nano-computing, descriptions such as 'computer system' or 'information system' will likely need to be interpreted as encompassing a greater range of devices.[84] In principle, however, the core concept of 'automated processing of information' would likely be sufficiently flexible to include, for instance, a monitoring and control smart chip with NFC and IP connectivity, built into a household appliance.

'Computer data' or 'computer information' is commonly described as a *'representation of facts, information or concepts that can be read, processed, or stored by a computer.'* Some approaches clarify that this includes a computer program.[85] Others are silent on the point. The difference between the formulations 'machine-readable' and 'can be read, processed or stored by a computer system (or information system)' is likely of a semantic nature only. In practice, computer data or information likely includes data or information stored on physical storage media (such as hard disk drives, USB memory sticks or flash cards), data or information stored in the memory of a computer system or information system, data or information transmissions (whether wired, optical, or radio frequency), and physical displays of data or information, such as in printout form or on a device screen.

While recognizing the use of different approaches to terminology, this Study makes use of the terms 'computer system' and 'computer data', which it treats as equivalent to 'information system' and 'computer information.'

Categories of cybercrime

While the term 'cybercrime' is not amenable to a single description, the question arises whether cybercrime objectives, features, or *modus operandi* can be identified in general terms, rather than (or in addition to) by reference to a list of individual cybercrime acts. As noted above, one

---

81 See, for example, Explanatory Report to the Council of Europe Cybercrime Convention, ETS No. 185.

82 A Guidance Note of the Council of Europe Cybercrime Convention Committee (T-CY) also reaches the conclusion that the definition of 'computer system' in Article 1(a) of the Council of Europe Cybercrime Convention covers developing forms of technology that go beyond traditional mainframe or desktop computer systems, such as modern mobile phones, smart phones, PDAs, tablets or similar. See Council of Europe. 2012. T-CY Guidance Note 1 on the notion of 'computer system.' T-CY (2012) 21, 14 November 2012.

83 COMESA Draft Model Bill, Part 1, Art. 1(b).

84 For a review of potential developments and regulatory challenges associated with the internet of things see European Union, 2009. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. *Internet of Things – An Action Plan for Europe*. COM (2009) 278 Final, 18 June 2009.

85 Council of Europe Cybercrime Convention, Art. 1(b).

example of this approach is found in the Commonwealth of Independent States Agreement, which describes an *'offence relating to computer information'* as a *'criminal act of which the target is computer information.'*[86] The Shanghai Cooperation Organization Agreement (more broadly) describes *'information offences'* as *'the use of information resources and (or) the impact on them in the informational sphere for illegal purposes.'* The Council of Europe Cybercrime Convention – although not by way of defined terms – uses broad criminalization headings, including *'offences against the confidentiality, integrity and availability of computer data and systems,' 'computer-related offences'* and *'content-related offences.'*[87] The Draft African Union Convention similarly uses criminalization chapter headings that make a distinction between *'offences specific to information and communication technologies'* and *'adapting certain offences to information and communication technologies.'*[88]

It is clear from these approaches that a number of general features could be used to describe cybercrime acts. One approach is to focus on the material offence *object* – that is, on the person, thing, or value against which the offence is directed.[89] This approach is seen in the Commonwealth of Independent States Agreement (where the offence object is computer information) and also in Title One of the substantive criminal law chapter of the Council of Europe Cybercrime Convention (where the objects are computer data or computer systems). Another approach is to consider whether computer systems or information systems form an integral part of the *modus operandi* of the offence.[90] This approach is also seen in Titles Two, Three and Four of the substantive criminal law chapter of the Council of Europe Cybercrime Convention, as well as in the Shanghai Cooperation Organization Agreement, and the Draft African Union Convention. Identifying possible cybercrime offence objects and *modus operandi* does not describe cybercrime acts in their entirety, but it can provide a number of useful general categories into which acts may be broadly classified.

Some international or regional instruments concern cybercrime only in the narrower conception of the computer system or data as the offence object.[91] Others address a broader range of offences, including acts where the offence object is a person or value, rather than a computer system or data – but where a computer system or information system is nonetheless an integral part of the *modus operandi* of the offence.[92] Chapter Four (Criminalization) examines the specific acts criminalized by such instruments in detail. While not all international or regional instruments use a broad conception of cybercrime, the approach taken by this Study aims to be as comprehensive as possible. It thus makes use of a wide list of cybercrime act descriptions, broadly organized in three categories based on the offence object and *modus operandi*. Due to the use of two methods of classification, some degree of overlap may exist between the categories.

---

86 Commonwealth of Independent States Agreement, Art. 1(a).

87 Council of Europe Cybercrime Convention, Titles 1, 2, and 3.

88 Draft African Union Convention, Part III, Chapter V, Section II, Chapters 1 and 2.

89 Those comprise offences against the confidentiality, integrity and availability of data and computer systems. See Calderoni, F., 2010. The European legal framework on cybercrime: striving for an effective implementation. *Crime, Law, and Social Change,* 54(5):339-357.

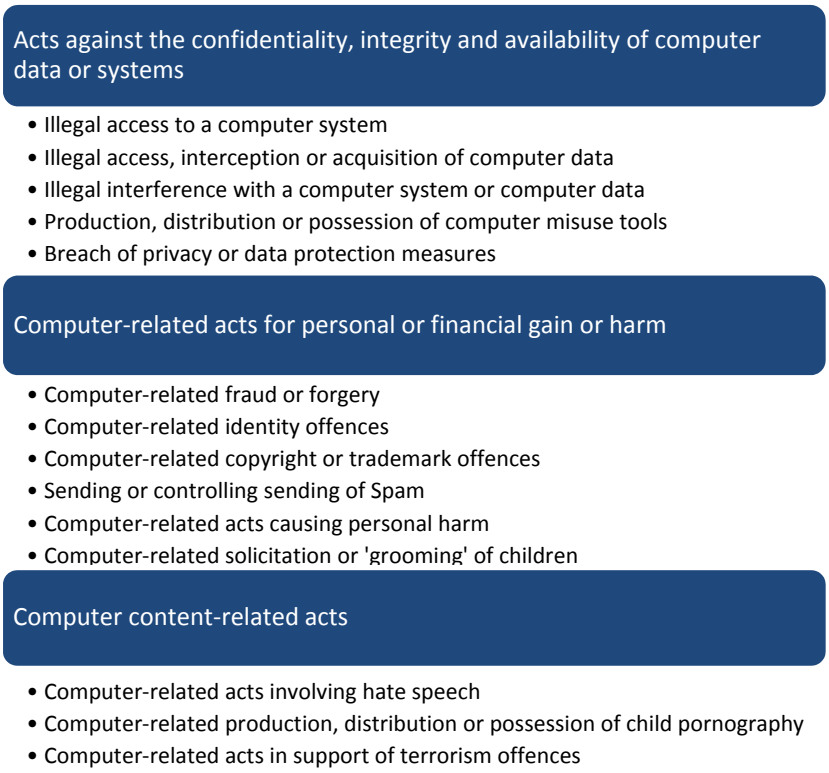
90 Podgor, E.S., 2002. International computer fraud: A paradigm for limiting national jurisdiction. *U.C. Davis Law Review*, 35(2):267-317, 273 et seq.

91 EU Decision on Attacks against Information Systems and Commonwealth of Independent States Agreement.

92 For instance, ECOWAS Draft Directive, Art. 17 (Facilitation of access of minors to child pornography, documents, sound or pornographic representation). See also Pocar, F., 2004. New challenges for international rules against cyber-crime. *European Journal on Criminal Policy and Research*, 10(1):27-37.

Acts constituting cybercrime

The figure below proposes 14 acts that may constitute cybercrime, organized in three broad categories. Annex One to this Study provides a more detailed description for each act. This list of acts was also used in the questionnaire sent to states, private sector entities, and intergovernmental and academic organizations for information gathering for the Study.[93] The purpose of the list is to introduce a tentative set of acts that may be included in the term 'cybercrime,' with a view to establishing a basis for analysis throughout the Study. The list is not intended to be exhaustive. In addition, the terms used – and the accompanying descriptions in Annex One – are not intended to represent legal definitions. Rather, they are broad 'act descriptions' that may be used as a starting point for analysis and discussion. While this Study does not 'define' cybercrime (either with a definition attached to the term itself, or by a 'definitive' list of acts), the conduct listed may nonetheless be considered as the basic content for the meaning of the term, at least for the purposes of this Study.[94]



It should be noted, at this stage, that the ubiquity of the internet and personal computer devices means that computer systems or computer data can be ancillary – at least in developed countries – to almost any criminal offence. Closely related to cybercrime therefore, but conceptually distinct, is the domain of electronic evidence. The collection and presentation of electronic evidence is integral to the investigation and prosecution of cybercrime. Increasingly this is also the case for conventional crimes such as robbery, theft, or burglary, as well as for forms of organized crime. Computerized telephone records, emails, IP connection logs, SMS messages, mobile telephone address books, and computer files may all contain evidence of the location,

---

93 The draft questionnaire for information gathering was developed initially by the Secretariat based on the list of topics for inclusion in the Study approved by the expert group on cybercrime (contained in *Report of the open-ended intergovernmental expert group on the comprehensive Study of the problem of cybercrime* (E/CN.15/2011/19)). The draft questionnaire, including a first draft of cybercrime act descriptions, was sent to all countries for comment in 2011. Following incorporation by the Secretariat of comments received, the final questionnaire, including the list of acts presented here, was approved by the Bureau of the Expert Group on Cybercrime at its meeting on 19 January 2012.

94 In response to comments from countries, a number of amendments have been made to the list of acts presented in this Chapter, compared to that used in the Study questionnaire. In the Study questionnaire, the second category was entitled 'Computer-related acts for personal or financial gain.' This has been amended to 'Computer-related acts for personal or financial gain or harm.' In the Study questionnaire, the third category was entitled 'Specific computer-related acts.' This has been amended to 'Computer content-related acts.' The items 'Computer-related acts causing personal harm' and 'Computer-related solicitation or 'grooming' of children' have been moved from the third category to the second category. In addition, the questionnaire contained the item 'Computer-related acts involving racism or xenophobia.' This has been amended to the broader category 'Computer-related acts involving hate speech.'

motive, crime scene presence, or criminal involvement of a suspect in almost any form of crime.

Acts against the confidentiality, integrity and availability of computer data or systems

The core list of cybercrime acts have as their object a computer system or computer data. Basic actions include unauthorized access, interception, acquisition, or interference with a computer system or data. Chapter Four (Criminalization) examines these further, both from a sample of national laws, and from international and regional instruments. These acts may be committed using many different *modus operandi*. Illegal access to a computer system, for example, may consist of the unauthorized use of a discovered password, or remote access using exploit software.[95] The latter may also constitute interference with computer data and/or a computer system. Individual acts can thus show a degree of overlap across offence 'baskets.' The first category also includes acts related to tools that can be used to carry out acts against computer systems or data.[96] Finally, the category includes criminal acts related to the (mis)handling of computer data in accordance with specified requirements.

'Operation Aurora'

In 2010, a series of online attacks were reported by several high-profile software companies, and, ultimately, breaches were recorded at a large search engine firm. Using a zero-day vulnerability in a web browser, the attackers created a tunnel into an internal network via employees' compromised workstations, and gained access to e-mail accounts and inadequately secured source code repositories.

The same year, users of a social networking site received e-mails from a fake account with links to a fictitious new login system appearing to be from the company, with the victim's username already entered in the login system. Users' credentials would then be compromised, and the infected host could potentially become a member of the ZeuS botnet.

Source: Trustwave. 2011. SpiderLabs Global Security Report.

Computer-related acts for personal or financial gain or harm

The second category focuses on acts for which the use of a computer system is inherent to the *modus operandi*. The object of such acts differs. In the case of computer-related fraud, the object may be considered as the economic property targeted. In the case of computer-related copyright or trademark offences, the offence object may be considered as the protected intellectual property right. In the case of computer-related acts causing personal harm, such as the use of a computer system to harass, bully, threaten, stalk or to cause fear or intimidation of an individual, or 'grooming' of a child, the offence object may be regarded as the individual targeted.

The '*Gozi*' virus

In early 2013, three European men were charged by North American prosecutors with the creation and distribution of a computer virus that infected more than a million computers worldwide, enabling them to access personal bank information and steal at least 50 million dollars in the period between 2005 and 2011. The virus was introduced in Europe and spread to North America, where it also infected computers belonging to national agencies. Extradition proceedings against two of the accused are under way. The case is said to be *'one of the most financially destructive yet seen.'*

Soure: http://www.fbi.gov/

The view that a diverse range of acts with different material offence objects can nonetheless

95 United Nations, 1994. *UN Manual on the Prevention and Control of Computer Related Crime.*

96 Examples include Low orbit ion cannon (LOIC), sKyWIper and the ZeuS banking malware.

be considered 'cybercrime' is supported by preliminary work on the development of a framework for an international classification of crimes for statistical purposes. Work by the Conference of European Statisticians notes that acts of 'cybercrime' could be recorded, for statistical purposes, by the use of an 'attribute tag' that would indicate the 'computer-facilitation' of a particular act within a (full) crime classification system. Such a 'tag' could apply, in principle, to computer-facilitated acts falling anywhere within the larger crime classification system – whether acts against the person, acts against property, or acts against public order or authority.[97]

A challenge concerning 'computer-related' cybercrime acts is that the category risks being expanded to include a broad range of otherwise 'offline' crimes, when committed with the use or help of a computer system. The question of whether this type of act should be considered 'cybercrime' remains somewhat open. While some international or regional instruments are limited to a comparatively few number of computer-related offences, others are expansive. The Council of Europe Cybercrime Convention, for example, covers (from this category) computer-related forgery and computer-related fraud alone.[98] In contrast, the League of Arab States Model Law contains criminal provisions on the use of a computer system for forgery, threats, blackmail, appropriating moveable property or a deed through fraudulent use of a name, unlawfully obtaining the numbers or particulars of a credit card, unlawfully benefiting from communication services, establishing an (internet) site with the intention of trafficking in human beings, narcotic drugs or psychotropic substances, and transferring illicit funds or disguising their illicit origin.[99]

Another act that may fit into this category – and, in contrast to those acts previously discussed, is exclusively cyber-related – is the sending and controlling of the sending of spam.[100] While the sending of spam is prohibited by all internet service providers, it is not universally criminalized by countries. Chapter Four (Criminalization) examines this area further.

Computer content-related acts

The final category of cybercrime acts concerns computer content – the words, images, sounds and representations transmitted or stored by computer systems, including the internet. The material offence object in content-related offences is often a person, an identifiable group of persons, or a widely held value or belief. In the same way as the second category, these acts could in principle be committed 'offline', as well as through the use of computer systems. Nonetheless, many international and regional cybercrime instruments include specific provisions on computer content.[101] One argument for the inclusion of content-related acts within the term 'cybercrime' is that computer systems, including the internet, have fundamentally altered the scope and reach of dissemination of information.[102]

---

97 See United Nations Economic Commission for Europe, Conference of European Statisticians. *Principles and Framework for an International Classification of Crimes for Statistical Purposes.* ECE/CES/BUR/2011/NOV/8/Add.1. 11 October 2011.

98 Council of Europe Cybercrime Convention, Arts. 7 and 8.

99 League of Arab States Model Law, Articles 4, 9-12, and 17-19.

100 Sending or controlling sending of spam refers to acts involving the use of a computer system to send out messages to a large number of recipients without authorization or request. See Annex One (Act descriptions).

101 See Council of Europe Cybercrime Convention, Art. 9; League of Arab States Convention, Art. 12 et seq.; and ITU/CARICOM/CTU Model Legislative Texts, Section II, among others.

102 Marcus, R.L., 2008. The impact of computers on the legal profession: Evolution or revolution? *Northwestern University Law Review,* 102(4):1827-1868.

The possession or dissemination of a range of content expressed via computer systems may be considered as criminal conduct by countries. In this respect, it is important to note that, in addition to the principle of state sovereignty, a key starting point enshrined in international human rights treaties is the right to freedom of opinion and expression.[103] From this starting point, international law *permits* certain necessary restrictions as provided for by law.[104] International law further *obliges* states to prohibit certain exceptional types of expression, including child pornography, direct and public incitement to commit genocide, forms of hate speech, and incitement to terrorism.[105] Chapter Four (Criminalization) examines national, international and regional approaches to the criminalization of computer content, including from an international human rights law perspective, in detail.

Conspiracy for preparation of a terrorist act

In May 2012, a Western European court sentenced one of its nationals to five years of imprisonment for participation in a criminal conspiracy for the preparation of a terrorist act. At trial, the prosecution presented dozens of decrypted e-mail communications of jihadist content, which were, among others, sent to the website of the President of the country, and traced back to a member of a globally operating extremist group. A preservation order enabled the authorities to identify communication between the extremist group's member and extremist websites, including a website with the stated goal of hosting and disseminating the extremist group's documents, audio and video recordings, statements from warlords and suicide attackers and the materials of other extremist groups. This indicated that the defendant actively performed, *inter alia*, the translation, encryption, compression and password-protection of pro-jihadist materials, which he then uploaded and circulated via the internet; and taking concrete steps to provide financial support to extremist group, including through the attempted use of PayPal and other virtual payment systems. The court found the required sufficient evidence to demonstrate that the defendant had provided not merely intellectual support, but also direct logistical support to a clearly identified terrorist plan.

Source: UNODC. 2012. Use of the internet for terrorist purposes.

Computer-related acts in support of terrorism offences are included in the content-related cybercrime category. The recent UNODC publication 'The use of the Internet for terrorist purposes'[106] observes that computer systems may be used for a range of acts that promote and support terrorism. These include propaganda (including recruitment, radicalization and incitement to terrorism); financing; training; planning (including through secret communication and open-source information); execution; and cyberattacks.[107] The questionnaire used for information gathering for this Study referred directly to computer-related incitement to terrorism, terrorist financing offences and terrorist planning offences.[108] As such, this Study concerns only on the computer *content* aspect of terrorism offences and excludes the threat of cyberattacks by terrorist organizations from the scope of the analysis – an approach equivalent to that of the UNODC publication on the use of the internet for terrorist purposes.

Other cybercrime acts

The list of 14 cybercrime acts is not exhaustive. During information gathering for the Study, countries were invited to identify other acts that they considered to also constitute cybercrime.[109] Responses included *'computer-related tools for facilitating illegal acts related to financial instruments and means of payment'*; *'online gambling'*; *'use of an information technology device for the purposes of trafficking in persons'*;

---

103 UDHR, Art. 19; ICCPR Art. 19; ECHR, Art. 9; ACHR Art. 13; ACHPR Art. 9.
104 Cassese, A., 2005. *International Law*. 2nd ed. Oxford: Oxford University Press. p.53. and pp.59 et seq.
105 United Nations General Assembly, 2011. *Promotion and protection of the right to freedom of opinion and expression. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.* A/66/290. 10 August 2011.
106 UNODC, 2012. *The Use of the Internet for Terrorist Purposes.* Available at https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf
107 *Ibid.*
108 Study cybercrime questionnaire. Act Descriptions section. See also Annex One (Act descriptions).
109 Study cybercrime questionnaire. Q39.

'computer-related drug trafficking'; *'computer-related extortion'*; *'trafficking in passwords'*; and *'access to classified information.'*[110] In all of these cases, respondents said that the act was covered by cyber-specific legislation – indicating the centrality of the use of computer systems or data to the act.

In some of these cases, the act may be considered as a specialized form or variation of one of the cybercrime acts already listed. Use or possession of computer-related tools for financial offences, for example, may be covered by the broad act of computer-related fraud or forgery.[111] Access to classified information may be a subset of illegal access to computer data in general. Trafficking in passwords is covered by some computer misuse tool provisions.[112]

Other acts, such as computer-related extortion,[113] raise the challenge of the inclusion (or non-inclusion) of offline crimes that have, to varying extents, migrated online – a point discussed briefly in the context of computer-related acts for personal or financial gain or harm. As noted by a number of responding countries, a general principle is frequently that *'what is illegal offline, is also illegal online.'*[114] In many cases, criminal laws regulating offline conduct can also be applied to online versions of the same conduct. Thus, countries have, for example, interpreted existing conventional laws to cover computer-related extortion,[115] or the use of computer systems to facilitate trafficking in persons.[116] National legal practice in this respect is examined further in Chapter Four (Criminalization).

The internet and illicit drug sales

Since the mid-1990s, the internet has increasingly been used by drug traffickers to sell illicit drugs or the chemical precursors required to manufacture such drugs. At the same time, illegal internet pharmacies advertise illicit sales in prescription medicines, including substances under international control, to the general public. These substances are controlled under the three international drug control treaties and include opioid analgesics, central nervous system stimulants, tranquillizers and other psychoactive substances. Many pharmaceuticals offered for sale in this way are either diverted from the licit market or are counterfeit or fraudulent – constituting a danger to the health of consumers. The fact that illegal internet pharmacies conduct their operations from all regions of the world and are able to relocate their business easily when a website is closed down means that taking effective measures in this area is essential.

In 2009, the International Narcotics Control Board (INCB) published 'Guidelines for Governments on Preventing the Illegal Sale of Internationally Controlled Substances through the Internet.' These Guidelines highlight the importance of: empowering appropriate authorities to investigate and take legal action against internet pharmacies and other websites, that are used in the illegal sale of internationally controlled substances; prohibiting shipment by mail of internationally controlled substances and ensuring that such shipments are intercepted; and establishing standards of good professional practice for the provision of pharmaceutical services via the internet.

One approach may be to include in a description of 'cybercrime' only those acts where the use of a computer system is strictly integral to fundamentally altering the scope or nature of the otherwise 'offline' act.[117] Drawing the line here is extremely challenging. Is it appropriate to argue,

---

110 *Ibid.*

111 Some countries, for example, include the act of 'possession of articles for use in frauds' within fraud criminal offences.

112 Computer passwords, access codes or similar data were not explicitly included in the act description for the item 'Production, distribution or possession of computer misuse tools' used in the Study questionnaire, leading some countries to identify this conduct as an additional act.

113 In addition to use of computer systems to communicate extortion-related threats, computer-related extortion can be associated with unauthorized interference with computer systems or data, such as demands for money linked to DDoS attacks.

114 Study cybercrime questionnaire. Q39.

115 See, for example, Landgericht Düsseldorf, Germany. 3 KLs 1/11, 22 March 2011, in which the accused was convicted of extortion and computer sabotage against online betting sites through the hired services of a botnet.

116 UN.GIFT, 2008. *The Vienna Forum to fight Human Trafficking. Background Paper for 017 Workshop: Technology and Human Trafficking.* Available at: http://www.unodc.org/documents/human-trafficking/2008/BP017TechnologyandHumanTrafficking.pdf
The UNODC trafficking in persons database also includes a number of cases involving the use of placement of online advertisements, https://www.unodc.org/cld/index.jspx For further information, please see also https://www.unodc.org/unodc/en/human-trafficking/what-is-human-trafficking.html?ref=menuside

117 This may be applied, for instance, in terms of sexual abuse of children, when images created by offenders 'offline' are subsequently

for example, that the use of computer systems is fundamentally a 'game-changer' when it comes to the nature and extent of consumer fraud, but not for trafficking in narcotic drugs? Is the use of online financial services to conceal the origin of criminal profit[118] significantly different from traditional financial transactions to require the definition of a separate offence of computer-related money-laundering? To some extent, the list of 14 acts presented in this Study represents an attempt to distil contemporary practice in terms of those acts that are commonly spoken of as 'cybercrime.'

Other acts referred to by countries, in particular online gambling, are not consistently criminalized across countries. The act of gambling through the internet is allowed in many countries, but is prohibited directly or indirectly in other countries.[119] Irrespective of its legal status, internet gambling sites may frequently be the subject or object of computer-related fraud or computer data interception or interference.[120] Within the general term 'online gambling', a distinction is sometimes made between the internet as a mere communication medium – akin to remote telecommunication gambling on a physical world event – and the case of a 'virtual' casino in which the player has no means of verifying the results of the game.[121] The latter, in particular, is often seen as distinct from offline gambling, due to its potential for compulsive engagement, fraud,[122] and abuse by minors. In accordance with the principle of national sovereignty, at least one regional approach recognizes the right for countries to set the objectives of their policy on betting and gambling according to their own scale of values and to define proportionate restrictive measures.[123] The inclusion of online gambling in a general description of cybercrime may thus face challenges concerning the universality of its criminalization.

Discussion

It is notable that responding countries did not identify a large range of conduct outside of the 14 cybercrime acts listed in the Study questionnaire. Some degree of consensus may therefore exist on at least a core of conduct included in the term 'cybercrime.'

Nonetheless, as discussed in this Study, the determination of whether it is necessary to include specific conduct in a description of 'cybercrime' depends, to a large extent, on the *purpose* of using the term 'cybercrime' in the first place.

From the international legal perspective, the content of the term is particularly relevant when it comes to agreements for international cooperation. One feature of international and regional cybercrime instruments, for example, is the inclusion of specialized investigative powers not usually found in non-cyber specific instruments.[124] States parties to instruments agree to make such powers available to other States parties through mutual legal assistance requests. While some

---

shared 'online' with networks of like-minded individuals – the additional acts of distributing, receiving and collecting the material 'online' are new criminal offences. An overview of this exemplified scenario and further examples can be found in: UK Home Office, 2010. *Cyber Crime Strategy*. p.45.

118 Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), 2012. *Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction*.

119 Fidelie, L.W., 2008. Internet Gambling: Innocent Activity or Cybercrime? *International Journal of Cyber Criminology*, 3(1):476-491; Yee Fen, H., 2011. Online Gaming: The State of Play in Singapore. *Singapore Academy of Law Journal*, 23:74.

120 See, for example, McMullan, J.L., Rege, A., 2010. Online Crime and Internet Gambling. *Journal of Gambling Issues*, 24:54-85.

121 Pereira de Sena, P., 2008. Internet Gambling Prohibition in Hong Kong: Law and Policy. *Hong Kong Law Journal*, 38(2):453-492.

122 See for example, European Court of Justice, *Sporting Exchange Ltd v Minister van Justitie*, Case C-203/08. para 34: '*Because of the lack of direct contact between consumer and operator, games of chance accessible via the internet involve different and more substantial risks of fraud by operators compared with the traditional market for such games*.'

123 *Ibid.* para 28.

124 Such powers include orders for stored computer data, real time collection of computer data, and expedited preservation of computer data. See, for instance, Draft African Union Convention, COMESA Draft Model Bill, Commonwealth Model Law, Council of Europe Cybercrime Convention, and League of Arab States Convention.

instruments have a broad scope that enables the use of such powers for the gathering of electronic evidence for *any* criminal offence,[125] others limit the scope of international cooperation and investigative powers to 'cybercrime', or 'offences relating to computer information.'[126] In the international sphere, conceptions of 'cybercrime' may thus have implications for the availability of investigative powers and access to extraterritorial electronic evidence. Chapter Seven (International cooperation) examines this area in detail.

As the world moves towards universal internet access, it may be that conceptions of cybercrime will need to operate on a number of levels: specific and detailed in the case of the definition of certain individual cybercrime acts, but sufficiently broad to ensure that investigative powers and international cooperation mechanisms can be applied, with effective safeguards, to the continued migration of offline crime to online variants.

125 See, for example, Council of Europe Cybercrime Convention and League of Arab States Convention.
126 See, for example, Commonwealth of Independent States Agreement and Draft African Union Convention.

CHAPTER TWO: THE GLOBAL PICTURE

Following a brief look at approaches to measuring cybercrime, this Chapter paints a global picture of 'who' (and how many) are involved in 'what' (and how much) cybercrime. It finds that cybercrime acts are broadly distributed across different cybercrime categories with victimization rates higher than conventional crime in many cases. While perpetrator profiles depend upon cybercrime act type, upwards of 80 per cent of cybercrime acts are estimated to originate in some form of organized activity.

2.1 Measuring cybercrime

Key results:

- Information sources for measuring cybercrime include police-recorded crime statistics; (population-based and business surveys; victim reporting initiatives; and technology-based cybersecurity information
- Statistics that purport to measure cybercrime as an aggregate phenomenon are unlikely to be comparable cross-nationally. Data disaggregated by discrete cybercrime act offers a higher degree of consistency and comparability
- While police-recorded cybercrime statistics are valuable for national-level crime prevention and policy making, they are not generally suitable for cross-national comparisons in the area of cybercrime. Survey-based and technology-based information source can, however, provide valuable insights
- Different information sources are used in this Study to address the questions of '*who*', '*what*' and '*how much*' cybercrime

Why measure cybercrime?

Article 11 of the United Nations Guidelines for the Prevention of Crime[1] states that crime prevention strategies, polices, programmes and actions should be based on a '*broad, multidisciplinary foundation of knowledge about crime problems.*' This 'knowledge base' should include the establishment of 'data systems.'[2] The collection of data for planning interventions to prevent and reduce crime is as important for cybercrime as it is for other crime types. Measurement of cybercrime can be used to inform crime reduction initiatives; to enhance local, national, regional and international responses; to identify gaps in responses; to provide intelligence and risk assessment; and to educate and inform the public.[3]

Many commentators highlight the particular challenges of collecting information on the

1 *Guidelines for the Prevention of Crime*, annex to United Nations Economic and Social Council Resolution 2002/13 on *Action to promote effective crime prevention,* 24 July 2002.
2 *Ibid.* Art. 21(f).
3 Fafinski, S., Dutton, W.H. and Margetts, H., 2010. *Mapping and Measuring Cybercrime.* Oxford Internet Institute Forum Discussion Paper No. 18., June 2010.

nature and extent of cybercrime.[4] These include the problem of determining what constitutes 'cybercrime' in the first place; challenges of under-reporting and under-recording; survey methodological and awareness issues; and possible conflicts of interest for private sector data.[5]

Which crimes should be measured?

The previous Chapter considered the possible content of the term 'cybercrime.' For the purposes of measurement, it is likely that acts within the first cybercrime category (acts against the confidentiality, integrity and availability of computer data or systems) and third category (computer content-related acts) can be relatively clearly delineated. The second category, however, (computer-related acts for personal or financial gain or harm) risks becoming extensive. As discussed, what would be the threshold for involvement of a computer system or data that warrants recording a crime as a cybercrime in this category? Approaches may differ in this respect, in particular as regards offences recorded by the police. The part below on police statistics discusses this challenge further.

Overall, it is clear that statistics that purport to measure 'cybercrime' as a *single phenomenon* are unlikely to be comparable cross-nationally, due to significant variations in the content of the term between recording systems. The preferred approach is therefore likely to be one that provides data disaggregated by *discrete cybercrime act* – such as those detailed in the list of 14 acts provided in Chapter One (Connectivity and cybercrime). Such an approach offers a higher degree of consistency and comparability, and is in line with good practice in crime and criminal justice statistics in general.[6]

What do we want to know?

One approach to the measurement of new forms and dimensions of crime, including cybercrime, is to aim to characterize '*who*' (and *how many*) are involved in '*what*' (and *how much*).[7] This requires a *combination* of data sources, such as: information on perpetrators, including organized criminal groups; information on flows within illicit markets; as well as information on numbers of criminal events, harms and losses, and resultant illicit financial flows. Each of these elements has implications for the response to cybercrime. An understanding, for example, of organized criminal group structures and networks is central to the design of criminal justice interventions. An understanding of illicit markets – such as the black economy centred on stolen credit card details – provides details of the underlying incentives for criminal activity (irrespective of the individuals or groups involved), and thus entry points for prevention programming. An understanding of the extent of harms, losses and illicit financial gains provides guidance on the prioritization of interventions.

What information can be gathered?

Four main information sources exist for the measurement of '*what*' cybercrime acts occur and '*how much*': (i) police-recorded crime statistics; (ii) population-based and business surveys; (iii) victim reporting initiatives; and (iv) technology-based cybersecurity information. The list is not

---

4 See, for example, Brenner, S.W., 2004. Cybercrime Metrics: Old Wine, New Bottles? *Virginia Journal of Law & Technology*, 9(13):1-52. Cybercrime is also included as an example of an 'emerging and difficult to measure crime' in documents of the 42nd Session of the United Nations Statistical Commission. See United Nations Economic and Social Council, Statistical Commission, 2012. *Report of the National Institute of Statistics and Geography of Mexico on Crime Statistics.* E/CN.3/2012/3, 6 December 2011.

5 Fafinski, S., Dutton, W.H. and Margetts, H., 2010. *Mapping and Measuring Cybercrime.* Oxford Internet Institute Forum Discussion Paper No. 18. June 2010.

6 See for example, UNODC, 2010. *Developing Standards in Justice and Home Affairs Statistics: International and EU Acquis;* and United Nations, 2003. *Manual for the Development of a System of Criminal Justice Statistics.*

7 European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI), 2011. Data Collection on [New] Forms and Manifestations of Crime. *In:* Joutsen, M. (ed.) *New Types of Crime, Proceedings of the International Seminar held in Connection with HEUNI's Thirtieth Anniversary*, 20 October 2011, Helsinki: EICPC. See also UNODC, 2010. *The Globalization of Crime: A Transnational Organized Crime Threat Assessment.*

exhaustive but covers the main sources of information that have some degree of cross-national comparability. Other sources include individual studies on selected phenomena, such as URL crawling techniques, or botnet takeover.[8] Annex Two to this Study examines the strengths and challenges associated with each source in turn. It finds that, at present, while police-recorded cybercrime statistics are valuable for national-level crime prevention and policy making, they are not generally suitable for cross-national comparisons in the area of cybercrime. In contrast, survey-based information and technology-based cybersecurity information is beginning to provide some insights into the nature and extent of the phenomenon. These information sources are used below to address the questions of '*what*' and '*how much*' cybercrime. The question of '*who*' is examined in the following section of this Chapter on cybercrime perpetrators.

2.2 The global cybercrime picture

Key results:

- Cybercrime acts show a broad distribution across financial-driven acts, computer-content related acts, as well as acts against the confidentiality, integrity and accessibility of computer systems
- Perceptions of relative risk and threat vary between Governments and businesses
- Individual cybercrime victimization is significantly higher than for 'conventional' crime forms. Victimization rates for online credit card fraud, identify theft, responding to a phishing attempt, and experiencing unauthorized access to an email account, vary between 1 and 17 per cent of the online population
- Individual cybercrime victimization rates are higher in countries with lower levels of development, highlighting a need to strengthen prevention efforts in these countries
- Private sector enterprises in Europe report victimization rates of between 2 and 16 per cent for acts such as data breach due to intrusion or phishing
- Criminal tools of choice for these crimes, such as botnets, have global reach. More than one million unique IP addresses globally functioned as command and control servers for botnets in 2011
- Internet content targeted for removal by governments includes child pornography and hate speech, but also defamation and government criticism, raising human rights law concerns in some cases
- Some estimates place the total global proportion of internet traffic estimated to infringe copyright at almost 24 per cent

This section paints a picture of the global nature and extent of cybercrime on the basis of data provided during information gathering for the Study from countries, private sector and academic organizations, as well as a review of over 500 open-source publications.[9]

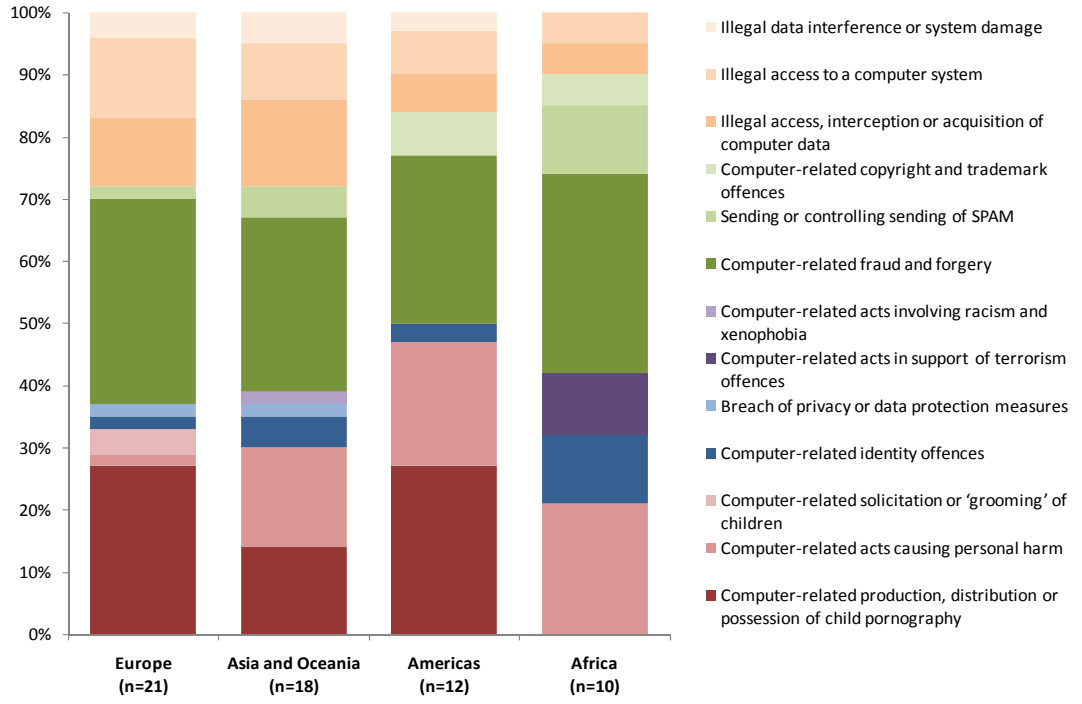
[8] See for example, Kanich, C. *et al.*, 2011. *No Plan Survives Contact: Experience with Cybercrime Measurement.* Available at: http://static.usenix.org/events/cset11/tech/final_files/Kanich.pdf ; see also Kemmerer, R.A., 2011. *How to Steal a Botnet and What Can Happen When You Do.* Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6080765

[9] Sources on file with the Secretariat.

Distribution of cybercrime acts

Cybercrime acts show a broad distribution across the range of offences. According to the perceptions of law enforcement institutions, *financial*-driven acts, such as computer-related fraud or forgery, make up around one third of acts across almost all regions of the world. A number of countries mentioned that '*fraud in electronic commerce and payment*', '*fraud on auction sites such as ebay,*' '*advanced fee fraud*', '*cybercrime targeting personal and financial information*' and '*fraud scheme through email and social networking sites*' were particularly prevalent.[10] As discussed below, the financial impact of such crime is significant.

Figure 2.1: Most common cybercrime acts encountered by national police



Source: Study cybercrime questionnaire. Q80. (n=61, r=140)

Another one third to, in some regions, half of acts relate to computer *content* – including child pornography, content related to terrorism offences, and content infringing intellectual property rights. Child pornography-related offences were identified more frequently in Europe and the Americas, than in Asia and Oceania or Africa – although this may relate to differences in law enforcement focus between regions, rather than underlying differences. Computer-related acts broadly 'causing personal harm,' on the other hand, were identified as more common in Africa, the Americas, Asia and Oceania, than in Europe. The discussion on content-related acts below further examines some of these trends.

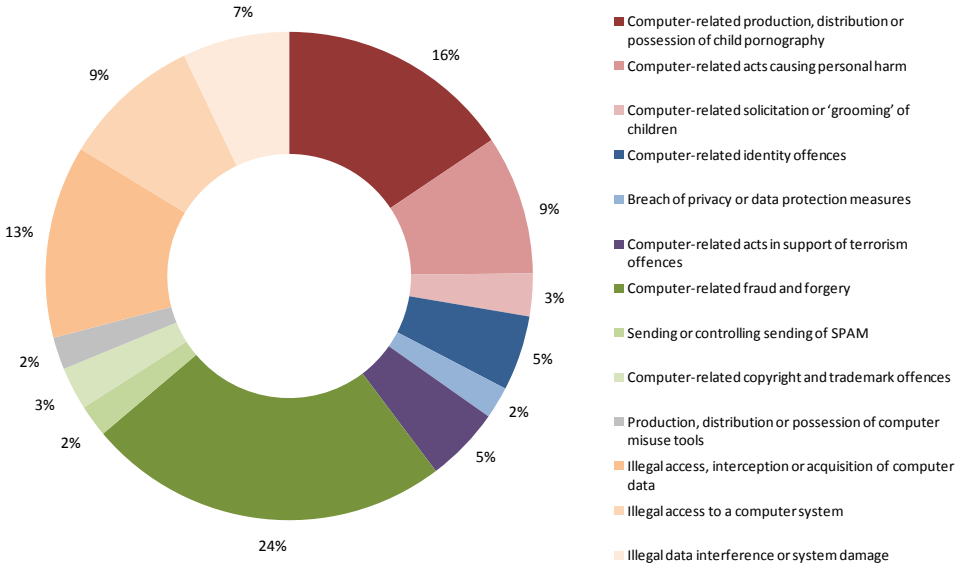
According to law enforcement perceptions, acts against the confidentiality, integrity and accessibility of computer systems, such as 'illegal access to a computer system', make up between one third and 10 per cent of acts, depending upon the region. Such actions are integral to a range of cybercrimes and it may be that differing capacities of countries to identify and to prosecute these (more technical) offences affects their perceived prevalence across regions. On the other hand, as discussed below, victimization surveys do suggest that there *are* differences in, for example, levels of

[10] Study cybercrime questionnaire. Q80 and Q85.

unauthorized computer access. These are not, however, always in the same direction as those perceived by law enforcement.

The theme that the prevalence and threat of cybercrime varies according to *who* is asked is well exemplified by comparison of results from countries and the private sector. When asked which cybercrime acts constitute the most significant *threat* (in terms of seriousness and loss or damage), the answers of law enforcement institutions were similar to those given regarding the most *common* acts – showing roughly equal distribution between financial-driven acts, content-related acts, and acts directly against computer systems or data.

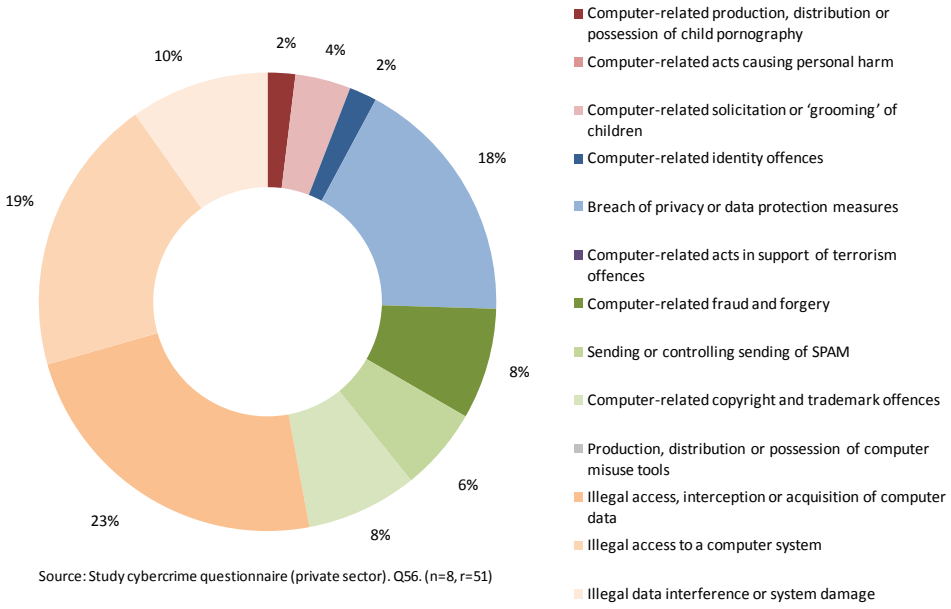
Figure 2.2: Most significant cybercrime threats - views of Member states



Source: Study cybercrime questionnaire. Q81. (n=59, r=138)

In contrast, as might be expected, private sector organizations viewed *acts against computer systems* as a significantly greater threat than other types of cybercrime. Illegal access, interference or damage are viewed by the private sector as a greater threat than all other types of cybercrime. This reflects a primary concern of private sector organizations for the confidentiality, integrity and accessibility of their computer systems and data.

Figure 2.3: Most significant cybercrime threats - views of private sector organizations



Source: Study cybercrime questionnaire (private sector). Q56. (n=8, r=51)

During information gathering for the Study, private sector organizations highlighted key cybercrime threats and risks, including '*unauthorized access to and exfiltration of intellectual property*';

'*intrusion to our web banking service*'; '*attempts to hack customer data systems*'; '*intrusion attacks*'; '*information leakage by employees*'; and '*denial of service attacks.*'[11] As discussed below, all private sector organizations are vulnerable to cyber-victimization and costs can be significant.

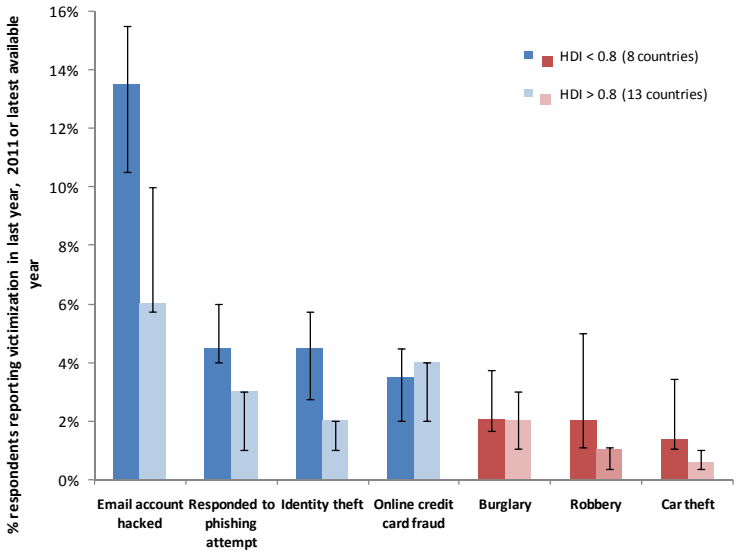
Prevalence and impact of cybercrime acts

Measurements of cybercrime act prevalence can be divided into general population (or consumer) victimization, and victimization of organizations – such as businesses, academic institutions, and others.[12]

Consumer victimization – For the general population, levels of cybercrime victimization are significantly *higher* than for 'conventional' offline forms of crime – with respect to the relevant populations at risk.[13] Cybercrime victimization rates for 21 countries across all regions of the world, for example, vary between one and 17 per cent of the online population for four specific acts: online credit card fraud; identity theft; responding to a phishing attempt; and experiencing unauthorized access to an email account.[14] In contrast, victimization surveys show that – for these same 21 countries – 'conventional' crime victimization rates, for burglary, robbery and car theft, vary between 0.1 and 13 per cent, with the vast majority of rates for these crimes under four per cent.[15] One factor responsible for this difference is likely the 'bulk' nature of many cybercrime acts. For acts such as phishing, or 'brute-forcing' email passwords to gain unauthorized access, a single individual can simultaneously target many victims in a way not possible in forms of conventional crime.

A second pattern is that cybercrime victimization rates (at least for the sample of 21 countries) are generally higher in those countries with *lower* levels of development. Dividing the countries into two groups – those with a human development index measurement lower than 0.8 (Group 1),

Figure 2.4: Cybercrime and conventional crime victimization



Source: UNODC elaboration of Norton Cybercrime Report and crime victimization surveys.

[11] Study cybercrime questionnaire (private sector). Q50-52 and Q56.
[12] Victimization of government institutions is excluded from the scope of this Study.
[13] All individuals for 'conventional' crime, and internet users for cybercrime.
[14] Symantec, 2012. *Norton Cybercrime Report 2012*. Research for the Norton Cybercrime Report was conducted independently by StrategyOne (now EdelmanBerland) through an online survey in 24 countries using identical questions translated into the primary language of each country. Interviews were conducted between 16 July 2012 and 30 July 2012. The margin of error for the total sample of adults (n=13,018) is +0.9 per cent at the 95 per cent level of confidence. Data from 3 countries in the Norton Cybercrime Report are excluded as national victimization data for conventional crime were not available. Victimization rates refer to 12 month prevalence of victimization.
[15] UNODC analysis of results from International Crime Victimization Survey (ICVS) and national crime victimization surveys. Victimization rates refer to 12 month prevalence of victimization.

and those greater than 0.8 (Group 2)[16] – shows higher victimization rates in the less developed countries (Group 1) for unauthorized access to an email account, identity theft, and responding to a phishing attempt. Online credit card victimization is slightly higher in the group of more developed countries. The figure shows the average victimization rate for these four cybercrime types, alongside average rates for burglary, robbery and car theft, for the two groups of countries.[17]

The pattern of higher cyber-victimization in less developed countries is consistent with generally higher conventional crime rates in less developed countries. For conventional crime, this difference is attributable to a number of factors, including income inequality, economic challenges, youthful populations, urbanization, a history of conflict, a proliferation of firearms, and poorly-resourced criminal justice systems.[18] Some of these factors have less relevance to cybercrime. Others, however, such as economic and demographic pressures, likely do form part of the cybercrime equation. Cyber-victims in lesser developed countries could, in principle, be targeted by perpetrators from anywhere in the world. Local cultural and language factors, however, can mean that potential victims are also targeted by perpetrators from their own country – making *national* perpetrator risk factors relevant. In addition, internet users in developing countries often face challenges of low cybersecurity awareness – making them especially vulnerable to crimes such as unauthorized access, phishing and identity theft.[19] This pattern also fits with the fact that – despite the pattern suggested by victimization surveys – law enforcement authorities in less developed countries do not identify illegal access-type cybercrime acts as particularly common.[20]

In contrast, online credit card fraud shows the opposite pattern. Victimization rates for this crime are broadly equivalent and possibly slightly higher in more developed countries. It is likely that this pattern is related in part to differences in credit card ownership and use online, as well as to differences in victim targeting due to perceptions of target worth. EUROPOL, for example, notes that high levels of 'card-not-present' credit card fraud affect EU credit cards, as a result of data breaches and illegal transactions.[21]

Widespread cybercrime consumer victimization carries with it significant financial costs – both direct and indirect. Direct and indirect costs include money withdrawn from victim accounts, time and effort to reset account credentials or repair computer systems, and secondary costs such as for overdrawn accounts. Indirect costs are the monetary equivalent of losses imposed on society by the existence (in general) of a particular cybercrime phenomenon. Indirect costs include loss of trust in online banking and reduced uptake by individuals of electronic services. The overall cost to society of cybercrime might also include 'defence costs' of cybersecurity products and services, as well as fraud detection and law enforcement efforts.[22]

Consumer victims of cybercrime in 24 countries across the world report that they suffered average direct losses of between 50 and 850 US dollars as a result of a cybercrime incident(s) experienced in one year.[23] Around 40 per cent of these costs were reported to consist of financial

---

16 Group 1: HDI mean=0.69, median=0.7; Group 2: HDI mean=0.89, median=0.90, The Human Development Index represents a combined measurement of social and economic development. See http://hdr.undp.org/en/statistics/hdi/

17 Averages are calculated as medians of victimization rates for each country group. Bars represent upper and lower quartiles.

18 See, for example, UNODC, 2005. *Crime and Development in Africa*; and UNODC, 2007. *Crime and Development in Central America.*

19 See, for example, Tagert, A.C., 2010. *Cybersecurity Challenges in Developing Nations.* Dissertation. Paper 22; and Grobler, M., et al., 2010. Evaluating Cyber Security Awareness in South Africa. *In*: Ottis, R. (ed.) 2011. *The Proceedings of the 10th European Conference on Information Warfare and Security*. Talinn: Cooperative Cyber Defence Centre of Excellence.

20 See above, for instance regarding information shown in Figure 2.4.

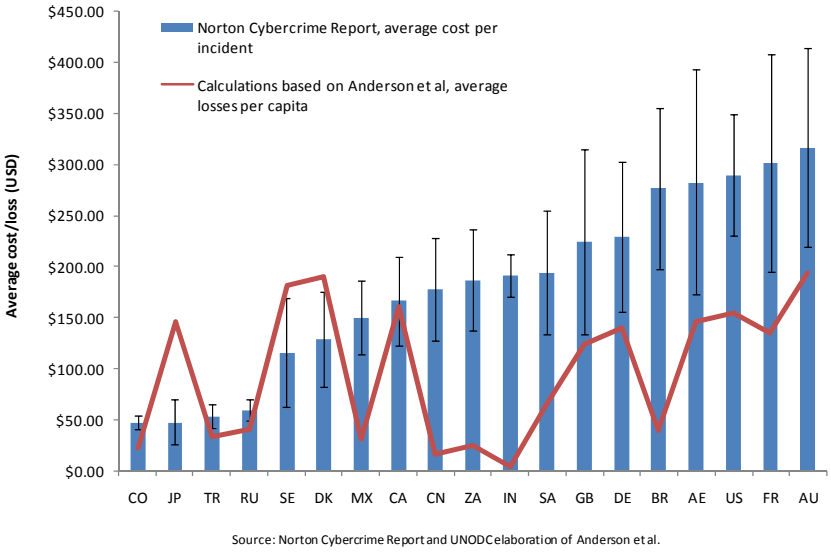
21 Europol, 2012. *Situation Report. Payment Card Fraud in the European Union. Perspective of Law Enforcement Agencies.*

22 See, for example, Anderson, R., et al., 2012. Measuring the Cost of Cybercrime. *11th Annual Workshop on the Economics of Information Security*, WEIS 2012, Berlin, 25-26 June 2012.

23 Symantec, 2012. *Norton Cybercrime Report 2012*. The survey question used asked all persons reporting any cybercrime victimization in the past 12 months how much they had lost financially over the past 12 months due to cybercrime. Respondents were asked to

loss due to fraud, almost 20 per cent due to theft or loss, 25 per cent to repairs, and the remainder to resolving the cybercrime or other financial loss.[24] Figure 2.5 shows average losses by country from this survey.[25] Differences in average reported loss across countries are likely due to a number of factors, including the type of cybercrime victimization, the effectiveness of cybersecurity measures, and the extent of victim use of the internet for online banking or payments. Costs estimated by victims themselves do not of course include indirect and defence costs.

Figure 2.5: Estimated costs of consumer cybercrime, by country



Source: Norton Cybercrime Report and UNODC elaboration of Anderson et al.

For comparison, the figure also shows estimated *total* costs of cybercrime (including direct, indirect and defence costs) per person, based on calculations from available literature.[26] The absolute *levels* of the two figures should not be compared – one is average direct costs per victim, the other represents total costs divided by the whole population. The *relative* patterns however do show some degree of correspondence. Where large differences arise, one contributing factor may be differences in internet penetration and distribution of costs across society. Dividing cybercrime losses across a large population that does not have access in its entirety to the internet – such as in less developed countries, for example – will have the effect of reducing apparent average losses *per capita*. This effect is clearly seen in the figure in the case of a number of developing countries, where the pattern for total estimated per capita losses does not well match the pattern for direct consumer reported losses. In such cases, it is likely that the underlying pattern is closer to that suggested by victim surveys. In contrast, in the case of highly developed countries with comparatively low consumer costs, estimated total losses per capita are higher than would be expected from consumer losses alone – alluding to additional significant indirect and defence costs in these countries.

Private sector victimization – Cybercrime techniques are revolutionizing traditional fraud and financial-driven offences committed against private sector organizations. Increasing criminal possibilities of not only defrauding an enterprise, but also of obtaining stored personal and financial information through data breach, have led to a significant perceived rise in private sector cybercrime

think about the total amount lost, including any amounts stolen and costs of repair and resolution. Total annual loss data was reported in local currency and converted to USD for cross-national comparison.

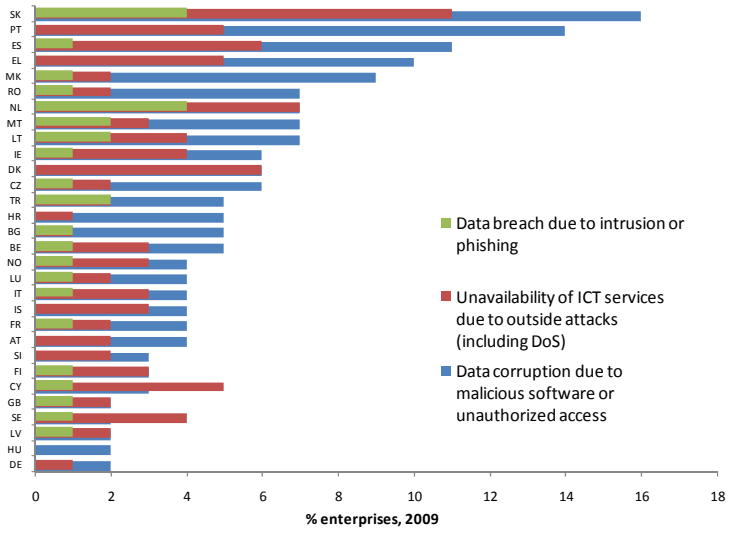
24 *Ibid.*

25 The figure excludes countries where the standard error in the estimate was greater than 0.5. This was the case, in particular, for some of the higher reported loss estimates.

26 UNODC calculations from Anderson, R., *et al.*, 2012. *Measuring the Cost of Cybercrime*. Global estimates from this source were attributed to countries based on GDP share.

risk.[27] At the same time, increased use of innovations such as cloud computing presents a mix of cybersecurity benefits and challenges.[28]

Figure 2.6: Cybercrime and enterprise victimization

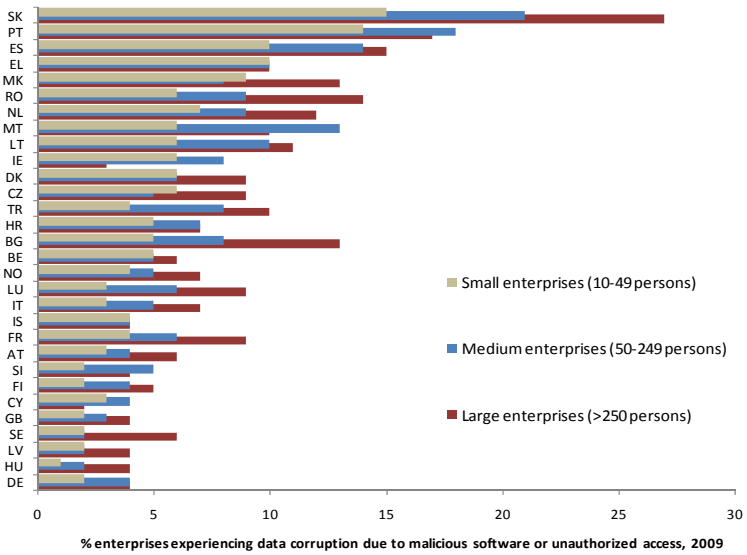


Source: Eurostat Community survey on ICT usage and e-commerce in enterprises.

Reliable private sector victimization data is hard to obtain and challenging to interpret.[29] Data for European countries nonetheless suggests that private sector cybercrime victimization rates for acts such as 'data beach due to intrusion or phishing', 'outside attacks resulting in system interference', and 'data interference due to illegal system access', are broadly comparable to unauthorized access, phishing and online credit card fraud experienced by consumers. Between two and 16 per cent of enterprises in Europe, for example, reported experiencing data corruption due to malicious software or unauthorized access during the year 2010.[30] Data corruption due to unauthorized access occurred more frequently than unavailability of ICT services due to outside attacks (between one and 11 per cent), which in turn occurred more frequently than data breach due to intrusion or phishing (between zero and four per cent).

Nonetheless, much turns on the way in which questions are asked, and the

Figure 2.7: Enterprise victimization by size



Source: Eurostat Community survey on ICT usage and e-commerce in enterprises.

27 See, for example, KPMG, 2011. *The e-Crime Report 2011*. Over half of enterprise security decision makers reported that the overall level of e-crime risk faced by their enterprise had increased over the last 12 months. Only 6 per cent reported that it had decreased. Europol reports that the main sources of illegal data in card-not-present fraud investigations were data breaches of merchants and card processing centres, often facilitated by insiders and malicious software (Europol, 2012. *Situation Report. Payment Card Fraud in the European Union. Perspective of Law Enforcement Agencies*).

28 PricewaterhouseCoopers, 2012. *Eye of the storm. Key findings from the 2012 Global State of Information Security Survey*.

29 See Annex Two (Measuring cybercrime).

30 Eurostat, 2011. *Community survey on ICT usage and e-commerce in enterprises*. The survey covered 149,900 enterprises out of 1.6 million in the EU27.

perception of respondents as to what constitutes a 'data breach', 'intrusion', 'unavailability of ICT services', or 'malicious software.' One survey covering private sector organizations in five countries, for example, reports extremely high enterprise 'victimization' rates – such as between 1.1 and 1.8 *'successful cyber-attacks per surveyed organization per week.'*[31] Such findings are likely heavily influenced not only by the perception of what constitutes a 'cyber-attack' on an enterprise,[32] but also by the *size* of the enterprise computer infrastructure available to attack. This particular survey, for instance, focused on organizations with more than 1,000 'enterprise seats' – defined as direct connections to the network and enterprise systems.[33]

Indeed, a greater cybercrime risk for larger enterprises is also borne out by data for the European private sector. The proportion of enterprises in Europe experiencing data corruption due to malicious software or unauthorized access is greater for large enterprises (more than 250 persons) (two to 27 per cent), than for medium enterprises (50-249 persons) (two to 21 per cent), which is, in turn, greater than for small enterprises (10-49 persons) (one to 15 per cent).

In addition to the 'available attack surface', such differences may also relate to a perception amongst perpetrators that larger enterprises represent higher value targets. It may also be the case, however, that small and medium enterprises possess a lower capacity to identify attacks in the first place. Some 65 per cent of large enterprises, for example, reported having a formally defined ICT policy, compared with 43 per cent of medium enterprises, and only 22 per cent of small enterprises.[34]

Criminal tools – the botnet

A defining feature of today's cybercrime landscape is the extensive use of computer misuse tools across a range of cyber-offences. 'Botnets' (a term derived from the words 'robot' and 'network') consist of a network of interconnected, remote-controlled computers generally infected with malicious software that turns the infected systems into so-called 'bots', 'robots', or 'zombies.'[35] The legitimate owners of such systems may often be unaware of the fact of infection. Zombies within the botnet connect to computers controlled by perpetrators (known as 'command and control servers' or C&Cs), or to other zombies, in order to receive instructions, download additional software, and transmit back information harvested from the infected system.

Because botnets can be used for a number of actions – including DDoS attacks, sending spam, stealing personal information, hosting malicious sites, and delivering 'payloads' of other malicious software[36] – they represent a key cybercrime tool of choice. A number of responding countries highlighted the increasing use of botnets in cybercrime during the past five years.[37] From a criminal law perspective, the installation of malware on a personal or enterprise computer system can represent illegal access to a computer system, and/or illegal data interference or system interference.[38] In countries where computer misuse tools are criminalized, producing, selling, possessing, or distributing botnet software itself may also be a criminal offence. In addition, use of the botnet for further criminal gain may constitute a range of offences, such as illegal access to,

---

31 HP/Ponemon, 2012. *Cost of Cybercrime Study AU, DE, JN, GB and US*.

32 Survey results are thus more reliable where experience of a particular, defined event, is asked about. See UNODC/UNECE, 2010. *Manual on Victimization Surveys*.

33 *Ibid.*

34 Eurostat, 2011. Statistics in Focus 7/2011. ICT security in enterprises, 2010.

35 OECD, 2008. *Malicious Software (Malware). A Security Threat to the Internet Economy*. DSTI/ICCP/REG(2007)5/FINAL. 28 April 2008.

36 Hogben, G. (ed.) 2011. *Botnets: Detection, Measurement, Disinfection and Defence*. European Network and Information Security Agency (ENISA).

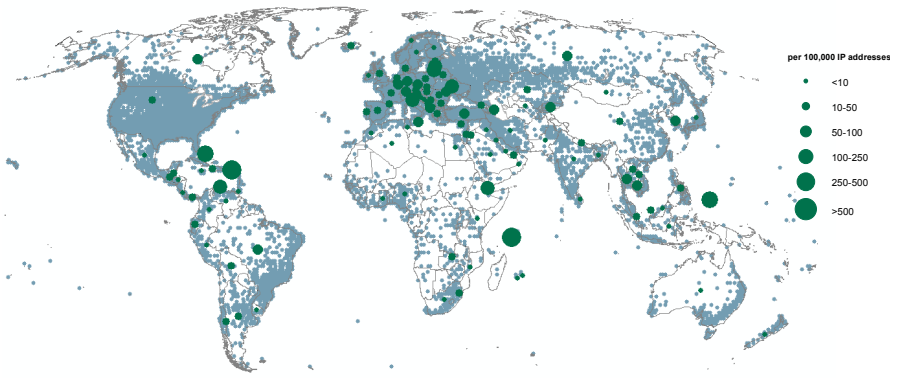
37 Study cybercrime questionnaire. Q84.

38 See Annex One (Act descriptions). See also NATO Cooperative Cyber Defence Centre of Excellence and ENISA, 2012. *Legal Implications of Countering Botnets*.

interception or acquisition of computer data; computer-related fraud; computer-related identity offences; or sending or controlling sending of spam.[39]

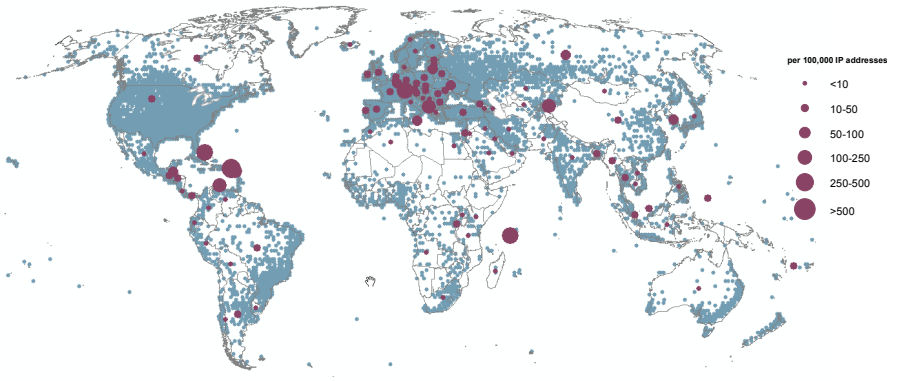
Mapping C&Cs and zombies – As botnets facilitate a wide range of cybercrime acts, an understanding of the location and extent of botnet C&Cs and zombies represents one important approach to characterizing 'global cybercrime.' Estimates suggest that more than *one million* unique IP addresses globally functioned at some point as a botnet C&C in 2011.[40] The distribution of identified C&Cs[41] is shown in Figures 2.8 and 2.9 for the years 2011 and 2012, per 100,000 country IP addresses.[42] In addition to a cluster of C&Cs in countries in Eastern Europe, numbers of C&Cs are high relative to the total number of country IP addresses in Western, Central and South-Eastern Asia, as well as in Central America and the Caribbean. While the *absolute* number of C&Cs is high in countries in North America, Western Europe and East Asia, relative C&C *rates* in these countries are low, due in part to the high number of internet connections and resultant IP addresses. Conversely, a small number of C&Cs in a country with limited connectivity may create a high C&C rate – in the same way as a few crimes on a small island can create a 'high' crime rate.

Figure 2.8: C&C servers, by country (2011)



Source: UNODC elaboration of data from Team Cymru.

Figure 2.9: C&C servers, by country (2012)



Source: UNODC elaboration of data from Team Cymru.

The global distribution of C&C servers is not necessarily linked with the location of perpetrators, or bot 'herders', who control C&Cs and their bots for the purposes of profit. The location of C&Cs servers can be moved often to avoid detection, and can include the use of

39 *Ibid.*

40 Estimate based on data from Team Cymru.

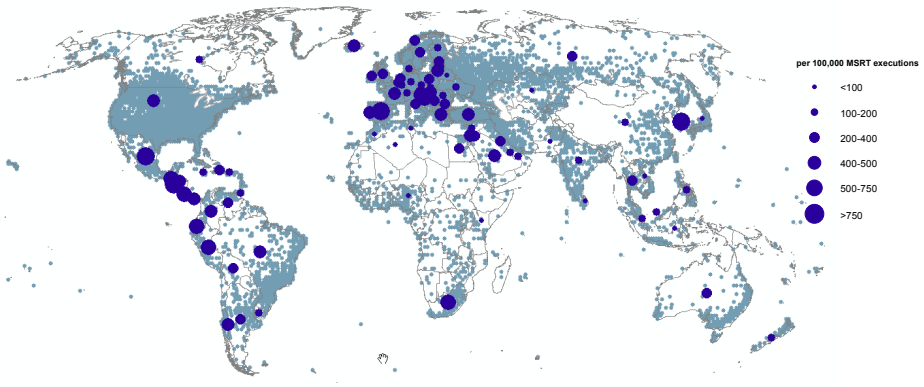
41 Data corresponds to IP addresses identified at any time during 2011 or 2012 as operating as an IRC (internet relay chat) or HTTP (hypertext transfer protocol) C&C server.

42 Data from Team Cymru. C&C rates per country are plotted in green (2011) and purple (2012), together with geolocation of all global IP addresses in blue (Data from MaxMind). Plotting identified C&Cs per 100,000 country IP addresses allows greater cross-national comparability than plotting of absolute C&C numbers. Geolocation of C&C IP addresses is subject to a number of challenges including use of proxy connections. Nonetheless location at country level is generally considered acceptable.

'innocent' compromised systems.[43] The bot herder need not therefore be located geographically close to his C&Cs. Nonetheless, it is possible that local – particularly linguistic – links exist between perpetrators and some hosting providers, including so-called 'bullet-proof' providers.[44] The section of this Chapter on 'cybercrime perpetrators,' for example, also notes the existence of perpetrator cybercrime hubs in Eastern Europe – corresponding with the pattern of high C&C rates in this sub-region.

Infected computers (zombies) are the other half of the equation to C&Cs. Globally, at least *seven million* computer devices may be part of a botnet.[45] Other estimates place the figure much higher.[46] Figure 2.10 shows approximate distribution of these infections, by country.[47]

Figure 2.10: Botnet infections, by country (2010)



Source: UNODC elaboration of Microsoft Security Intelligence Report.

Infection distribution shows a different pattern to that of C&Cs. Zombies cluster more heavily in Western Europe (as opposed to Eastern Europe for C&Cs), and show significant infection rates in North, Central and Southern America, as well as some countries in Eastern Asia. This distribution tends to represent countries with high numbers of active computer users.

Estimates of total zombies and botnet size face significant limitations. Two important methodological distinctions affecting estimates include botnet '*footprint*' versus '*live population*',[48] and measurement of zombie '*IP addresses*' versus '*unique devices.*'[49] In this respect, it should be noted that (due to methodological factors) the C&C estimate above concerns unique *IP addresses*, whereas the zombie estimate concerns computer *devices*. The two global figures are thus not easily comparable.

---

43 In addition, in more recent P2P botnets, any *zombie* computer can be a client or a server, precluding the need for a particular server for bots to download programs or receive instructions.

44 With respect to hosting providers see, for example, HostExploit and Group IB, 2012. *Top 50 Bad Hosts and Networks Report.*

45 UNODC calculations based on Microsoft, 2010. *Microsoft Security Intelligence Report.* Volume 9. Figure as of first half 2010. This estimate is of the same order of magnitude as that of Symantec, 2011. *Internet Security Threat Report. 2011.* Volume 17 (estimate of 4.5 million for 2010).

46 See, for example, Acohido, B., 2010. Are there 6.8 million –or 24 million– botted PCs on the Internet? *The Last Watchdog.* Available at: http://lastwatchdog.com/6-8-million-24-million-botted-pcs-internet/

47 Zombies are plotted as bot infections identified per 100,000 runs of the Microsoft Malicious Software Removal Tool. Data from Microsoft, 2010. *Microsoft Security Intelligence Report.* Volume 9. The methodology covers only those machines running Windows update (approximately 600 million machines worldwide) and identifies only the most wide-spread bot infections. Nonetheless, independent methodologies find similar infection levels when calculated on an individual country basis. See, for example, van Eeten, M.J.G. *et al.*, 2011. *Internet Service Providers and Botnet Mitigation. A Fact-Finding Study on the Dutch Market.* Faculty of Technology Police and Management, Delft University of Technology.

48 Zombies join and leave botnets on a continuous basis as new machines are infected and existing zombies cleaned. In addition, infected machines may suffer from multiple infections or be temporarily migrated from one botnet to another (Abu Rajab, M., et al., 2007. My Botnet is Bigger than Yours (Maybe, Better than Yours): Why size estimates remain challenging). *Proceedings of the first conference on first workshop on hot topics in understanding botnets.* Berkeley, CA: Usenet Association. The botnet *footprint* refers to the aggregated total number of machines that have been compromised over time. The botnet *live population* denotes the number of compromised machines that are simultaneously connecting with a C&C server.

49 A particular number of identified IP addresses does not usually correspond to the number of *devices* due to two network effects: (i) the short-term assignment of different IP addresses to the same device (DHCP 'churn'), and (ii) the sharing of a single IP address by multiple devices (NAT). Depending upon the size of DHCP and NAT effects, the number of unique IP addresses may be greater or smaller than the corresponding number of actual devices. Due to high DHCP churn rates by commercial ISPs, the number of observed IP addresses is usually significantly greater than the number of devices.

Indeed, when it comes to estimates of individual botnet size, the common technique of reporting unique zombie *IP addresses* measured over long periods of time is likely to significantly overestimate the number of infected devices.[50] While botnet size measurements remain controversial, evidence suggests that 'successful' bot herders typically control groups of infected computers of the order of *tens or hundreds of thousands* of devices – rather than the frequently reported 'millions' of devices.[51] On this basis, the total number of large criminal 'commercial' botnets globally is likely comparatively small. In addition, however, a much higher number of small, 'amateur' botnets, consisting of low zombie populations, may also exist.[52]

Example of information harvested by botnets: 'Torpig'

- C&C domains controlled by academic researchers for a period of 10 days
- 183,000 zombie devices identified during 10 days. Average 'Live' zombie population at any one time of 49,000. Most zombies likely in Northern Europe and North America
- Victim *credentials* for 8,300 accounts at 400 different financial institutions sent to C&C server
- Details of 1,700 credit cards sent to C&C server
- 298,000 victim *usernames and passwords* for webmail and social networking sites sent to C&C server
- Sufficient aggregate bandwidth of zombies to launch a massive DDoS attack

Source: Stone-Gross *et al.*

The harm – Such malicious networks are nonetheless capable of significant harm. During one single 10 day period, a botnet of around 183,000 zombie devices was found to harvest almost 310,000 items of victim bank account, credit card, and webmail and social networking credentials.[53] As discussed in the section in this Chapter on 'cybercrime perpetrators,' the potential of botnets to harvest such information has been instrumental in the development of cybercrime criminal 'markets' based largely on botnet sale and rental.[54] As noted in the 2010 UNODC Transnational Organized Crime Threat Assessment, the market in personal information harvested through botnets can be largely divided – with different individuals focused on collecting volumes of financial and identifying information, selling it on, and 'cashing it out.'[55]

Content offences

Overview – One third to one half of the most common cybercrime acts concern content-related offences.[56] Content may be regulated by criminal law for a range of reasons, including where contrary to national security, public safety, public order, health or morals, or the rights and freedoms of others.

Globally, information from over 4,600 requests by national authorities for removal of content from Google services shows that a wide range of material is perceived by governments to impinge upon these areas.[57] Not all such material may strictly engage the criminal law. Nonetheless,

---

50 It is likely that IP address based measurements only correspond well to the number of infected devices when reported over short time scales, such as one hour. Unique IP addresses measured over longer periods significantly overestimate the number of devices due to DHCP churn. In one botnet study, 1.25 million unique zombie IP addresses identified over 10 days corresponded only to 183,000 bots according to unique bot-ID (Stone-Gross, B., et al. 2009. Your Botnet is My Botnet: Analysis of a Botnet Takeover. In: *16th Annual ACM Conference on Computer and Communications Security (CCS)*, 9-13 November 2009). In addition, zombie counts are affected by the 'no-see' time before a device or IP address is considered to no longer be a member of the botnet (see http://www.shadowserver.org/wiki/pmwiki.php/Stats/BotCounts).

51 See, for example, http://www.secureworks.com/cyber-threat-intelligence/threats/waledac_kelihos_botnet_takeover/; http://www.secureworks.com/cyber-threat-intelligence/threats/The_Lifecycle_of_Peer_to_Peer_Gameover_ZeuS/; Stone-Gross, B., et al. 2009. Your Botnet is My Botnet: Analysis of a Botnet Takeover. CCS '09.

52 See, for example, http://www.symantec.com/connect/blogs/botnets-masses

53 Stone-Gross, B., *et al.*, 2009. Your Botnet is My Botnet: Analysis of a Botnet Takeover. CCS '09.

54 See, for example, Panda Security, 2010. *The Cybercrime Black Market: Uncovered.*

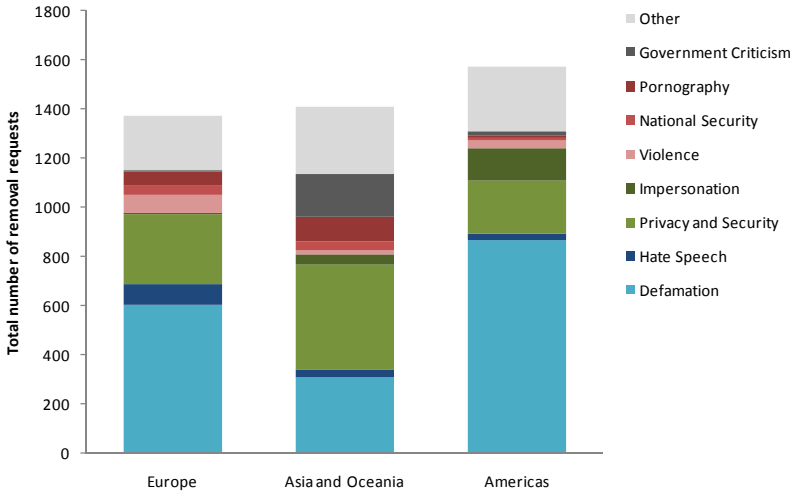
55 UNODC, 2010. *The Globalization of Crime. A Transnational Organized Crime Threat Assessment.*

56 See above, Section 2.2 The global cybercrime picture, Distribution of cybercrime acts.

57 Data from www.google.com/transparencyreport

figure 2.11 demonstrates that content involving violence; privacy and security concerns; impersonation; hate speech; defamation; and government criticism is considered a target for removal from the internet. The total number of removal requests is comparable across regions. For all regions, removal requests most commonly involve material related to defamation, and privacy and security. Linked with this pattern, during information gathering for the Study, a number of countries in Northern Africa and South-Eastern Asia noted cybercrime trends of *'more and more frequent use of social networks for defamation and propaganda,'* as well as '*an upward trend in acts related to reputation and privacy*' and '*libellous online postings.*'[58] As discussed in Chapter Four of this Study (Criminalization), while online global content cannot be judged in terms of a single morality, a high threshold is demanded when the tool of criminal law is used to limit freedoms of expression.[59]

Figure 2.11: Content removal requests received by Google from governments 2010-2012



Source: UNODC elaboration of Google Transparency Report.

Child pornography – One content type which may – indeed, must – be subject to criminal measures, however, is child pornography. During information gathering for the Study, acts involving child pornography were reported to constitute almost one third of the most commonly encountered cybercrimes for countries in Europe and the Americas. The proportion was lower – at around 15 per cent – for countries in Asia and Oceania.[60] Since 2009, almost 1,000 unique commercial child pornography websites have been identified, each with its own distinctive name and 'brand.' Some 440 of these were active during 2011.[61] Each website is a gateway to hundreds or thousands of individual images or videos of child sexual abuse. They are often supported by layers of payment mechanism, content stores, membership systems and advertising. Recent developments include the use of sites that when loaded directly display legal content, but when loaded via a particular referrer gateway site enable access to child pornography images. In addition, single law enforcement operations against P2P filesharing of child pornograpy have identified IP addresses to the order of millions offering child pornography.[62]

Intellectual property infringement – Intellectual property rights are the rights given to persons over the creations of their minds. They usually give the creator an exclusive right over the use of his or her creation for a certain period of time. Almost all materials in which such rights vest can conceivably be made available online – whether literary or artistic works, sound recordings, distinctive signs such as trademarks, details of inventions protected by patents, industrial designs or

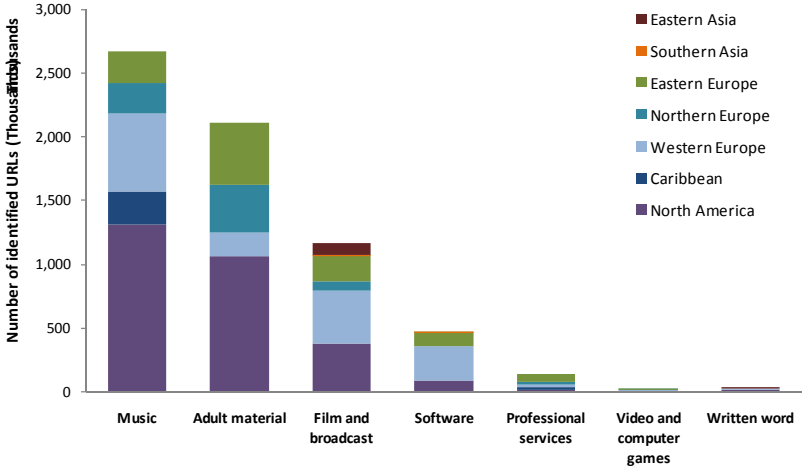
58 Study cybercrime questionnaire. Q81 and Q85.
59 See Chapter Four (Criminalization), Section 4.3 International human rights law and criminalization, Limitations on freedom of expression and international law.
60 Study cybercrime questionnaire. Q81.
61 Internet Watch Foundation, 2011. *Annual Report 2011.*
62 See http://www.justice.gov/psc/docs/natstrategyreport.pdf

trade secrets. When these rights are infringed – such as by unlawful copying or use – the means of enforcement usually lies in civil proceedings between individuals with, in certain cases, the right to bring private criminal prosecutions. In addition, in some circumstances, the state may have the right to initiate criminal proceedings. Generally, international agreements such as TRIPS specify that countries shall provide for *criminal* procedures and penalties at least in cases that are '*committed wilfully and on a commercial scale.*'[63]

Identifying the nature and extent of computer-related, or online, *criminal* intellectual property right infringement is therefore far from simple. The best that can be done, on a global scale, is to identify how much – and what type of – material likely *infringes* property rights overall. Depending upon the context and circumstances – including scale, intent, purpose, and applicable law and jurisdiction – a certain proportion of individuals involved in such infringing use may then be subject to criminal sanctions.

Copyright – as the right protecting books, writings, music, films and computer programs – has particular relevance to online content. Globally, some estimates suggest that almost *24 per cent* of total internet traffic infringes copyright.[64] The level of infringing traffic varies by internet 'venue,' being highest in areas such as P2P services or 'cyberlocker' download sites, that are commonly used for distribution of films, television episodes, music, computer games and software.[65] Analysis of requests concerning over 6.5 million URLs by copyright holders for removal of infringing content from Google services gives some insight into the distribution of the *type* of material, and *location* of the *hosting site*.[66] Copyright holders most often requested removal of infringing music, followed by adult material, film and broadcast and computer software. Other forms of content were the object of a considerably lower number of requests. The majority of sites hosting this material were located in North America and Europe, although the Caribbean also featured for sites hosting infringing music.

Figure 2.12: Copyright removal requests received by Google from top 60 copyright owners, by content type and location of identified website 2011-2012



Source: UNODC elaboration of Google Transparency Report

While this information cannot be used to ascertain *criminal* intellectual property infringement, it is notable that some individual removal requests concern multiple URLs, sometimes

63 TRIPS, Art. 61.

64 Envisional, 2011. *Technical report: An Estimate of Infringing Use of the Internet. January 2011*. This estimate excludes all pornography, the infringing status of which can be difficult to discern.

65 *Ibid.*

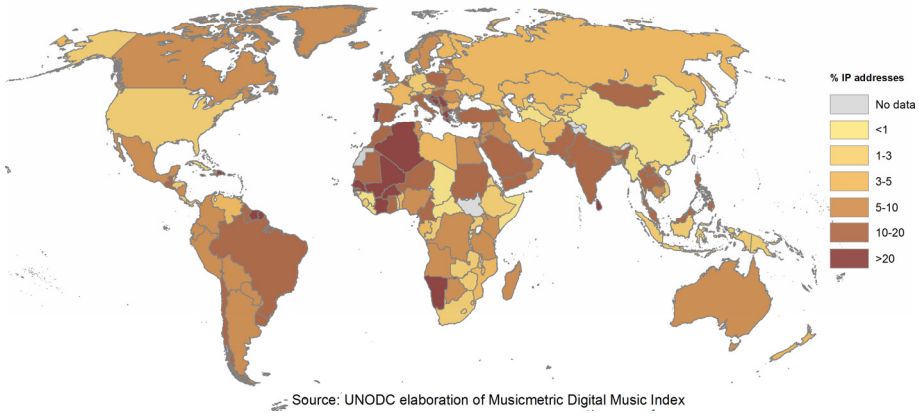
66 The analysis is restricted to the top 60 requesting copyright holders by number of URLS requested for removal. Results from removal requests received by Google are influenced both by the nature and extent of infringing material and the propensity of rights holders to actively seek for infringing material and to request removal.

of the order of tens of thousands, identified at a single domain.[67] Indeed, criminal actions have been commenced against individuals responsible for websites hosting large amounts of allegedly infringing material that are similar to others included in the Google removal request data.[68]

Detailed global information on downloads from one P2P file-sharing service, BitTorrent, shows the distribution of *use* of internet services that may be used to share infringing material. Total BitTorrent traffic is estimated to account for 18 per cent of *all* internet traffic. Nearly two-thirds of this traffic is estimated to be non-pornographic copyrighted content such as films, television episodes, music, and computer software.[69]

The map shows the percentage of total country IP addresses uniquely identified as downloading music by one of 750,000 tracked artists from BitTorrent in the first half of 2012.[70] For these artists, during this period, some 405 million music releases were downloaded through BitTorrent – almost 80 per cent albums and just over 20 per cent singles.[71] The download pattern shows that, relative to the number of country IP addresses, downloads were particularly high in countries in Africa, South America, and Western and South Asia.

Figure 2.13: Unique music downloads from BitTorrent, by country (1H 2012)



Source: UNODC elaboration of Musicmetric Digital Music Index

Such activity may not meet typical thresholds for criminal intellectual property rights infringement. Nonetheless, during information gathering for the Study, a few countries in the Americas and Africa indicated that computer-related copyright and trademark offences were a common cybercrime concern. One country in Southern Africa noted, for example, that '*one of the most common kind of cybercrime acts which represents a significant threat is the unlawful production of artistic work which leads to an increase in fake goods in the market.*'[72] In general, however, responses from the Study questionnaire showed that private sector organizations tended to view intellectual property-related cybercrime as a greater threat than countries did.[73] Perhaps surprisingly, however, computer-related copyright and trademark offences featured significantly less prominently for the private sector than a range of other possible cybercrime acts, such as breach of privacy or data protection measures, or illegal data or system interference.[74]

67 See http://www.google.com/transparencyreport/removals/copyright/
68 See http://www.justice.gov/opa/pr/2012/January/12-crm-074.html
69 Envisional, 2011. *Technical report: An Estimate of Infringing Use of the Internet. January 2011.*
70 UNODC elaboration of data from MusicMetric. Digital Music Index. See www.musicmetric.com/dmi
71 *Ibid.*
72 Study cybercrime questionnaire. Q81.
73 See above, Section 2.2 The global cybercrime picture, Distribution of cybercrime acts.
74 *Ibid.*

2.3 Cybercrime perpetrators

Key results:

- Cybercrime perpetrators no longer require complex skills or techniques, due to the advent and ready availability of malware toolkits
- Upwards of 80 per cent of cybercrime acts are estimated to originate in some form of organized activity, with cybercrime black markets established on a cycle of malware creation, computer infection, botnet management, harvesting of personal and financial data, data sale, and 'cashing out' of financial information
- Cybercrime often requires a high degree of organization to implement, and may lend itself to small criminal groups, loose *ad hoc* networks, or organized crime on a larger scale. The typology of offenders and active criminal groups mostly reflect patterns in the conventional world
- In the developing country context in particular, sub-cultures of young men engaged in computer-related financial fraud have emerged, many of whom begin involvement in cybercrime in their late teenage years
- The demographic nature of offenders mirrors conventional crime in that young males are the majority, although the age profile is increasingly showing older (male) individuals, particularly concerning child pornography offences
- While some perpetrators may have completed advanced education, especially in the computer science field, many known offenders do not have specialized education
- There is a lack of systematic research about the nature of criminal organizations active in cyberspace; and more research is needed regarding the links between online and offline child pornography offenders

As set out in the section in this Chapter on 'Measuring cybercrime', characterization of a crime typically requires information on '*who*' (and *how many*) are involved in '*what*' (and *how much*).[75] This section examines the perpetrator '*who*' component, with a focus on typical offenders and likely levels of criminal organization. It does so, in particular, with reference to the crimes of computer-related fraud, and computer-related production, distribution or possession of child pornography.

The full depiction of a 'cybercrime perpetrator' may contain many elements. Age, sex, socio-economic background, nationality, and motivation are likely amongst the core characteristics.[76] In addition, the level of criminal organization – or the degree to which individuals act in concert with others – represents a defining feature of the human association element behind criminal conduct.[77] Understanding cybercrime as a 'socio-technological' phenomenon, based on an appreciation of the characteristics of persons who commit such crimes, represents a broader approach to prevention than that focused solely on technical cybersecurity concepts.[78]

---

75 European Institute for Crime Prevention and Control, affiliated with the United Nations (HEUNI), 2011. Data Collection on [New] Forms and Manifestations of Crime. *In*: Joutsen, M. (ed.) *New Types of Crime, Proceedings of the International Seminar held in Connection with HEUNI's Thirtieth Anniversary*, 20 October 2011, Helsinki: EICPC. See also UNODC, 2010. *The Globalization of Crime: A Transnational Organized Crime Threat Assessment.*

76 United Nations Department of Economic and Social Affairs, Statistics Division, 2003. *Manual for the Development of a System of Criminal Justice Statistics.* ST/ESA/STATSER.F/89.

77 Levi, M., 1998. Perspectives on 'Organised Crime': An Overview. *The Howard Journal*, 37(4):335-345.

78 Yip, M., Shadbolt, N., Tiropanis, T. and Webber, C., 2012. *The Digital Underground Economy: A Social Network Approach to Understanding Cybercrime.* Paper presented at the *Digital Futures* conference, 23-25 October 2012, Aberdeen.

While individual characteristics are comparatively straightforward to define, it is well known that analysis of organized crime frequently presents both definitional and measurement challenges. This Study adopts the broad definition of the United Nations Organized Crime Convention of an organized criminal group.[79] Within this definition, various approaches to typologies exist,[80] as well as approaches to classifying a particular criminal offence as 'organized crime.'[81] There is no reason to think that the development of such typologies and approaches cannot in some way be applied to the involvement of organized criminal groups in cybercrime – albeit with some fresh challenges, and determined on a case-by-case basis.[82] Indeed, one key proposition of the EUROPOL Internet Facilitated Organised Crime Threat Assessment (iOCTA) is that '*the structure of cybercrime groups marks the cleanest break to date from the traditional concept of organized crime groups as hierarchical.*'[83] This section finds that while this may be true in many cases, it is necessary to consider a broad range of typologies, including taking into account online/offline criminal activity dynamics.

'Typical offender' profiles

Information on individual offender profiles is most commonly gained from retroactive studies of cohorts of prosecuted cybercrime cases. Undercover law enforcement operations on online underground forums, as well as perpetrator observation work by academic researchers in discussion forums and chat rooms also represent a valuable source of information. Additional approaches include the use of anonymous self-report questionnaires, observation at IT 'underground security' events, and the deployment of internet-connected 'honey-pots.'[84] Comparison of

Cybercrime suspects identified by police (A country in Southern Asia)

In one country in Southern Asia, published national police statistics contain details of recorded cybercrime offences and suspects. Suspects are classified in reported statistics through a number of categories, according to relationship with the victim and other characteristics. While a high proportion of suspects remain unclassified, national police statistics show that:

- Over 10 per cent of recorded cybercrime suspects are known to the victim as neighbours, friends, or relatives;
- 'Disgruntled employees' and 'crackers' each constitute around 5 per cent of recorded cybercrime perpetrators;
- A significant number of cybercrime suspects are enrolled in higher education and other learning programmes.

Source: http://ncrb.gov.in/

79 Under Article 2 of the Organized Crime Convention; '*an 'Organized criminal group' shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit.'* Article 2(c) clarifies that '*a 'Structured group' shall mean a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure.'*

80 One UNODC typology of organized criminal groups consists of: (i) 'Standard hierarchy' (single hierarchical group with strong internal systems of discipline); (ii) 'Regional hierarchy' (hierarchically structured groups, with strong internal lines of control and discipline but relative autonomy for regional components); (iii) 'Clustered hierarchy' (a set of criminal groups which have established a system of coordination/control, ranging from weak to strong, over all their activities); (iv) 'Core group' (a relatively tightly organized but unstructured group, surrounded in some cases by a network of individuals engaged in criminal activities); and (v) 'Criminal network' (a loose and fluid network, often drawing on individuals with particular skills, who constitute themselves around an ongoing series of criminal projects. UNODC, 2002. *Results of a Pilot Survey of Forty Selected Organized Criminal Groups in Sixteen Countries. September 2002.*

81 Europol, for example, has specified that for any crime or criminal group to be classified as "organized crime" at least six of the following characteristics must be present, four of which must be those numbered (1), (3), (5) and (11): (1) collaboration of more than two people; (2) each with his or her own appointed tasks; (3) for a prolonged or indefinite period of time; (4) using some form of discipline and control; (5) suspected of the commission of serious criminal offences; (6) operating on an international level; (7) using violence or other means suitable for intimidation; (8) using commercial or businesslike structures; (9) engaged in money laundering; (10) exerting influence on politics, the media, public administration, judicial authorities or the economy; and (11) determined by the pursuit of profit and/or power. Europol Doc. 6204/2/97. ENFOPOL 35 Rev 2.

82 Even though, for example, the individual and institutional custodians of compromised computers in a botnet may be unwitting participants in a criminal enterprise, some commentators maintain that botnets should be considered a form of organized crime. (Chang, L. Y. C., 2012. *Cybercrime in the Greater China Region.* Cheltenham: Edward Elgar).

83 Europol, 2011. *Internet Facilitated Organised Crime Threat Assessment (Abridged).* iOCTA. File No. 2530-264.

84 See, for example, Chiesa, R., Ducci, S. and Ciappi, S., 2009. *Profiling Hackers. The Science of Criminal Profiling as Applied to the World of Hacking.* Boca Raton, FL: Taylor & Francis Group.

studies is complicated by differences in methodology; cybercrime acts included; sample selection, geographic coverage; and approaches to analysis and presentation of perpetrator characteristics – such as the use of different perpetrator age intervals. This section presents data both on studies that profile cybercrime perpetrators across a broad range of offences, and those that focus on particular acts – such as illegal access to computer systems or data, and computer-related production, distribution or possession of child pornography.

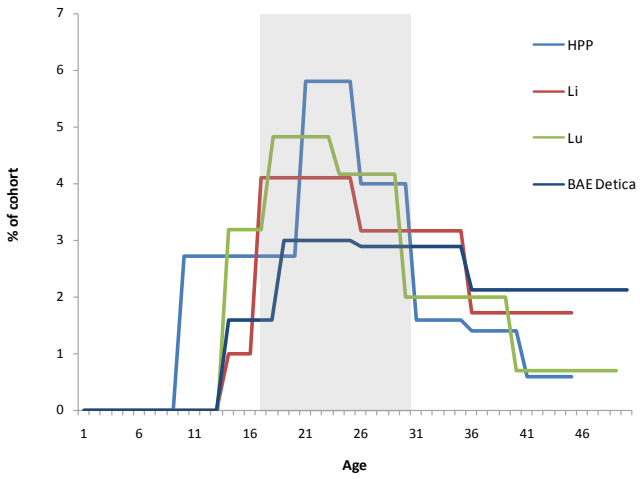
Use of a legal business as a cybercrime front

Two principal organizers of a group of about 30 people based in Eastern Europe supplied legal computer server and hosting services. Through this licit activity they concealed hundreds of 'smswarez' (illegal trade in content protected by copyright in return for payment by SMS), 'smswebs' (webpages where copyright-protected content can be downloaded in return for payment by SMS) and 'torrents.' The organizers used spam to advertise these illicit services, which ultimately led to the seizure of 48 illegal servers with a capacity of 200-250 terabytes. After this group was arrested national internet data turnover was reduced by about 10 per cent.

UNODC Digest of Organized Crime Cases

The analysis below is derived from three key studies[85] that cover a range of cybercrime acts, as well as from a self-report questionnaire study focusing on hackers.[86] The 'Li' cohort corresponds to 151 offenders in 'typical' cybercrime cases prosecuted by a country in North America between 1998 and 2006.[87] The 'Lu' cohort consists of over 18,000 cybercrime suspects recorded in the police database of a territory in Eastern Asia between 1999 and 2004.[88] The 'BAE Detica' study examined two samples of 250 distinct reported organized 'digital' crime group activities from a global literature review. In contrast, the 'HPP' hacking study relies on data from around 1,400 self-report questionnaires completed by 'hackers' – who may, or may not, have been involved in any crime.[89]

Figure 2.14: Age groups of cybercrime perpetrators



Source: UNODC elaboration of HPP, Li, Lu and BAE Detica

Age – Figure 2.14 shows perpetrator age groups from the four studies.[90] All studies suggest that cybercrime perpetrators are most commonly aged between 18 and 30 years. Li, for example, finds 37 per cent of perpetrators between the age of 17 and 25 years. Lu finds 53 per cent of perpetrators between the age of 18 and 29 years.

85 Li, X., 2008. The Criminal Phenomenon on the Internet: Hallmarks of Criminals and Victims Revisited through Typical Cases Prosecuted. *University of Ottawa Law & Technology Journal*, 5(1-2):125-140, ('Li'); Lu, C.C., Jen, W.Y., Chang, W. and Chou, S., 2006. Cybercrime & Cybercriminals. *Journal of Computers*, 1(6):1-10, ('Lu'); and BAE Systems Detica and London Metropolitan University, 2012. *Organised Crime in the Digital Age* ('BAE Detica').

86 UNICRI and Chiesa, R., 2009. *Profiling Hackers.* Available at: http://www.unicri.it/emerging_crimes/cybercrime/cyber_crimes/docs/profiling-hackers_add-info.pdf ('HPP').

87 The Li cohort included hacking/illegal access, attack, sabotage, viruses, data theft/espionage, and computer-related identity theft, fraud, embezzlement and corruption.

88 The Lu cohort included internet fraud, cyber piracy, computer misuse, and computer-related money laundering, pornography, sex trading, gambling, and larceny.

89 Commentators note that popular culture conceptions of 'hackers' that are not well defined or established have been used to fill cybercrime perpetrator 'information gaps.' See Wall, D. 2012. The Social Construction of Hackers as Cybercriminals. *In:* Gregoriou, C. (ed), *Constructing Crime: Discourse and Cultural Representations of Crime and 'Deviance'.* Houndsmills, UK: Palgrave Macmillan, p.4-18.

90 As the studies report perpetrator ages using different intervals, results are graphed by assuming equal distribution across the reported age intervals. Underlying data for each study likely show variation within each age interval.

The more recent BAE Detica study differs somewhat, in that it indicates possible higher levels of continued offending amongst persons in their 30s and 40s – with 32 per cent of perpetrators reported to be between the age of 36 and 50 years. In contrast to studies that include a range of cybercrime acts, the HPP hacking study shows a sharper decline in older perpetrator age groups – with only 21 per cent of all perpetrators above the age of 30 years. This may fit with the identification of sub-profiles of hackers that start at a young age – such as 'script kiddies.' The HPP finds, for example, that 61 per cent of hackers reported starting between the ages of 10 and 15 years. Cybercrime perpetrators overall may, in turn, be younger than criminal offenders in general. In the East Asian territory examined by Lu, the peak age group for total crime perpetrators was found to be 30 to 39 years, compared with 18 to 23 years for cybercrime perpetrators.

Gender – Cybercrime perpetrators are overwhelmingly male – the HPP, Li and Lu studies found 94, 98 and 81 per cent male perpetrators, respectively. Findings of more than 90 per cent correspond to a higher proportion of male involvement in cybercrime than for crime in general. Globally, the proportion of males prosecuted for any crime is typically between 85 and 90 per cent, with a median of around 89 per cent.[91] This pattern fits with data provided by countries during information gathering for the Study. One country in Northern Europe, for example, commented that '*perpetrators are young and male*.'[92]

Few studies have been carried out in developing countries that provide a clear picture covering all ages. Nonetheless, sub-profiles of cybercrime perpetrators such as 'yahooboys'[93] confirm at least the particular engagement of young men in cybercrime activities. One such study finds that 50 per cent of such perpetrators in one country in Western Africa are aged 22 to 25 years – with more than half claiming to have already spent five to seven years in cybercrime.[94]

Technical skill – With respect to the level of technical skill and knowledge of cybercrime perpetrators, the majority of the cases analysed by Li did not involve complex skills or techniques unavailable to common computer users. Overall, 65 per cent of all acts were relatively simple to achieve, 13 per cent required medium level skills and 22 per cent were complicated. The most complex attacks were those involving viruses, worms, and spyware – of which 73 per cent were classified as complicated. As commonly highlighted by cybersecurity organizations, it is likely that the possibility of purchasing computer tools able to

Profile of student 'yahooboys' in a country in Western Africa

Age	
<22 years	5 per cent
22-25 years	50 per cent
26-29 years	40 per cent
>29 years	5 per cent
Sex	
Male	95 per cent
Female	5 per cent
Number of years spent in cybercrime	
<2 years	2.5 per cent
2-4 years	35 per cent
5-7 years	55 per cent
>7 years	7.5 per cent
Parents' level of education	
None	2.5 per cent
Primary	5 per cent
Secondary	12.5 per cent
Tertiary	80 per cent

Aransiola, J.O. and Asindemade, S.O. 2011. Understanding Cybercrime Perpetrators and the Strategies they employ. *Cyberpsychology, Behaviour and Social Networking*. 14(12), 759-763.

91 HEUNI and UNODC, 2010. *International Statistics on Crime and Justice*. Helsinki: HEUNI.

92 Study cybercrime questionnaire. Q85.

93 The sub-culture of '*yahooboys*' describes youths, especially those living in cities, who make use of the internet for acts of computer-related fraud, phishing and scamming. Adeniran, A.I., 2011. Café Culture and Heresy of Yahooboyism. *In:* Jaishankar, K. (ed.) *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour.* Boca Raton, FL: CRC Press, Taylor & Francis Group.

94 Aransiola, J.O., and Asindemade, S.O., 2011. Understanding Cybercrime Perpetrators and the Strategies they employ. *Cyberpsychology, Behaviour and Social Networking*, 14(12):759.

exploit computer vulnerabilities and hijack large numbers of computers means that cybercrime perpetrators no longer require high levels of technical skill.[95] Skill levels are therefore likely to be highly variable[96] and – as discussed below – this may itself play some role in cybercrime group structure. Overall, however, education levels amongst cybercrime perpetrators may still be higher than for conventional, or all, crime. The Lu study found 28 per cent of cybercrime suspects in the territory had undertaken tertiary education, compared with eight per cent for all crime. Similarly, the HPP study found that more than half of hackers had undertaken tertiary education. Nonetheless, as noted by the BAE Detica study, it is likely that the 'artificial' acquisition of technical skills (such as through malware toolkits including ZeuS or the Butterfly Bot) has resulted in a shift away from the traditional profile of a highly-skilled digital criminal, towards a much wider pool of individuals.

Child pornography perpetrators

The profile of persons engaged in the computer-related production, distribution or possession of child pornography may be different to that of cybercrime perpetrators in general. Recent information on this perpetrator group has been gathered by the 'Virtual Global Taskforce' (VGT)[97] in the form of a small non-random sample of 103 persons arrested for downloading and exchanging child pornography through online P2P services.[98]

Age and social status – All suspects in the VGT cohort were male and ranged in age from 15 to 73 years, with an average age of 41 years. One in five suspects was not working but was retired, unemployed, or receiving health-related welfare benefits. The others were working or studying. 42 per cent were living with a partner and/or children. These perpetrators were significantly older (average of 50 years) than single offenders (average of 35 years). All suspects were concerned with hiding their activities from others, but 60 per cent succeeded in separating it completely from their daily life. For the rest of the group, their offending activities tended to become obsessive, were more or less enmeshed with their daily life, and possibly not well hidden from others. This latter group tended to be of low socio-economic status and to be highly computer literate and around 4 per cent of offenders reported a mental health problem.

Offending patterns – Suspects tended to have been involved in child pornography offending for a comparatively long period – an average of five years, ranging from six months to 30 years. Over 60 per cent of suspects not only collected child pornography but also traded/distributed it through a P2P network, and 35 per cent were involved in network(s) other than P2P. Of those, half participated in 'offline' networks – suggesting that individuals who go beyond accessing child pornography to trading it do so not only online, but also offline.

Links with 'offline' offending – As between 'online' and 'offline' offenders, online offenders are more likely to be Caucasian, unemployed and marginally younger than offline offenders.[99] Links nonetheless may exist.[100] One recent meta-study found that in a sample of over 3,500 online child

---

95 See, for example, Symantec, 2011. *Report on Attack Kits and Malicious Websites*; Fortinet, 2013. *Fortinet 2013 Cybercrime Report – Cybercriminals Today Mirror Legitimate Business Processes*; and Trend Micro, 2012. *The Crimeware Evolution.*

96 The HPP, for example, found that hacker technical skills were distributed as follows: low (21 per cent); medium (32 per cent); high (22 per cent); expert (24 per cent).

97 The Virtual Global Taskforce For Combating Online Child Sexual Abuse is an international partnership between nine law enforcement agencies established in 2003. See www.virtualglobaltaskforce.com

98 Because of the small size of the sample and its non-random case selection process, findings are not generalizable to the population of online offenders. Nonetheless, some insights into the characteristics of these individuals and their offending can be gained. See Bouhours, B. and Broadhurst, R., 2011. *Statistical Report: Virtual Global Taskforce P2P Online Offender Sample July 2010–June 2011.* Canberra: Australian National University. Available at: SSRN: http://ssrn.com/abstract=2174815 or http://dx.doi.org/10.2139/ssrn.2174815

99 Babchishin, K., Hanson, R. and Herrmann, C., 2011. The Characteristics of Online Sex Offenders: A Meta-Analysis. *Sex Abuse: A Journal of Research and Treatment*, 23(1):92-123.

100 See for example, Broadhurst, R. and Jayawardena, K., 2007. Online Social Networking and Paedophilia: An Experimental Research 'Sting.' *In:* Jaishankar, K., ed. *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior.* Boca Raton, FL: CRC Press, 79-102;

pornography offenders, one in six were also involved in 'offline' abuse of children.[101] In the VGT study, six per cent had previously been charged with online child sex offending, 18 per cent had previously been charged with a contact offence involving a child younger than 16 years and 15 per cent had been charged with previous non-sexual offending. There was little overlap between prior sexual and non-sexual offending, suggesting that suspects tended to specialize in child sex offending. Suspects with the deepest involvement in online child pornography activities were also those most likely to have engaged or currently engage in child sexual abuse.[102]

Overall, offenders in the VGT sample had a relatively high rate of previous and concurrent child offline sexual abuse offending. For over half the suspects with prior child sexual abuse charges, there was also evidence of current engagement in child sexual abuse. Because of the small VGT sample size and potential selection bias, however, it is not possible to answer the question of whether men who engage in online child pornography offences are at greater risk of also engaging in 'real life' sexual offending against children. This represents an important direction for future research.

Role of organized criminal groups

Many cybercrime acts require a high degree of organization and specialization, and it is likely that the level of involvement of conventional organized criminal groups in cybercrime is high – at least in financial-driven cybercrime acts such as computer-related fraud, forgery and identity offences. It must be remembered, however, that estimates of the '*proportion of cybercrime cases related to organized crime*' are influenced, in particular, by the definitions of 'cybercrime' and 'organized crime' applied, and – in particular – by the distribution of different cybercrime acts within any cohort examined. Acts involving child pornography, for example, may have a low involvement of 'organized crime' if individual downloaders are *not* viewed as acting in a 'structured group' for the 'commission of an offence.'

Online gambling by a traditional mafia family

In 2008, 26 individuals – including reputed mafia organized crime family members – were indicted on charges of operating a sophisticated illegal gambling enterprise, including four gambling websites in a country in Central America. The District Attorney commented that 'law enforcement crackdowns over the years on traditional mob-run wire rooms have led to an increased use by illegal gambling rings of offshore gambling websites where action is available around the clock.' While gambling was illegal in the prosecuting jurisdiction, the websites took advantage of different legislation in other jurisdictions. Bets were placed in the country but processed offshore and the data 'bounced' through a series of server nodes to evade traditional law enforcement detection methods.

Please see http://www.fbi.gov/newyork/press-releases/2012/four-gambino-crime-family-members-and-associates-plead-guilty-in-manhattan-federal-court

Elliot, A., Beech, A.R., Mandeville-Norden, R. and Hayes, E., 2009. Psychological Profiles of Internet Sexual Offenders: Comparisons with Contact Sexual Offenders. *Sex Abuse: A Journal of Research and Treatment*, 21(1):76-92; Endrass, J., Urbaniok, F., Hammermeister, L.C., Benz, C., Elbert, T., Laubacher, A. and Rossegger, A., 2009. The Consumption of Internet Child Pornography and Violent and Sex Offending. *BMC Psychiatry*, 9:43-49; Webb, L., Craissati, J., Keen, S., 2007. Characteristics of Internet Child Pornography Offenders: A Comparison with Child Molesters. *Sex Abuse: A Journal of Research and Treatment*, 19:449-465.

101 Wolak, J., Finkelhor, D., Mitchell, K., 2011. Child Pornography Possessors: Trends in Offender and Case Characteristics. *Sex Abuse: A Journal of Research and Treatment*, 23(1):22-42. Another study focusing on child pornography offenders, the 'Butner Study', was carried out comparing groups of offenders participating in voluntary treatment, on the basis of whether they had an additional documented history of 'hands-on' sexual offences against at least one child. The study's results *'highlight[ed] the fact that the relationship between viewing child pornography and contact sexual criminality is a complex interaction.'* It was found that the online offenders *'were significantly more likely than not to have sexually abused a child via a hands-on act,'* and that *'many [of them] may be undetected child molesters, and that their use of child pornography is indicative of their paraphilic orientation.'* If not for their online criminal activities, *'these offenders may not otherwise have come to the attention of law enforcement.'* See: Bourke, M.L., Hernandez, A.E., 2008. The 'Butner Study' Redux: A Report of the Incidence of Hands-on Child Victimization by Child Pornography Offenders. *Journal of Family Violence*, 24:183-191.

102 Bouhours, B., Broadhurst, R., 2011. *Statistical Report: Virtual Global Taskforce P2P Online Offender Sample July 2010–June 2011.* Canberra: Australian National University.

Moreover, the application of current models of organized crime to 'online' activity is not without its challenges. Traditional features of organized crime such as the use of violence and control of territory are difficult to translate to cybercrime activity. In addition, issues of traditional 'governance' of organized criminal groups, including trust and enforcement, may not be easily mediated in an environment of online forums or chat rooms. Nonetheless, what individuals can do, organizations can also do – and often better. The internet and related technologies lend themselves well to broader coordination between individuals across a dispersed area – opening up possibilities for shorter-lived 'swarm' criminal associations, and divergence from traditional models such as standard and regional hierarchy-based groups.[103] As discussed below, in a relatively short period of time, cybercrime has transformed from a low volume crime committed by an individual specialist offender to a common high volume crime, '*organized and industrial like.*'[104]

One recent study that reviewed a sample of 500 recorded cybercrime offences, estimated that upwards of 80 per cent of digital crime may now entail some form of organized activity.[105] An upper estimate for organized crime involvement in cybercrime may be 90 per cent.[106] The EUROPOL iOCTA claims that where not already the case, in the near future the '*vast majority*' of investigations into transnational organized crime will necessitate some form of internet investigation. Although purposefully biased towards organized crime cases, the UNODC Digest of Organized Crime Cases concludes that the presence of an organized criminal group as a constant factor in all cybercrime cases examined '*substantially diminishes the role of isolated hackers as main actors in cybercrime.*'[107] The Digest also notes that the nature of cybercrime offences '*necessarily requires the organization of many means and human resources.*'

A number of responding countries also mentioned an increasing involvement of organized criminal groups in cybercrime during the last five years. One country in Western Africa, for example, noted the '*development of cybercrime groups that are more and more organized and possessing a transnational dimension.*' A country in South America stated '*cybercrime went from an offence committed by an isolated criminal to crime committed by criminal organizations,*' and a country in South-Eastern Asia concluded '*cybercrime has become syndicated with respective individuals engaged in different specialized roles.*'[108]

Organized criminal groups can therefore be considered, at the very least, as *significant cybercrime actors*. The limited empirical evidence nonetheless requires caution – regarding conclusions both as to the proportion of organized crime involvement, and its form and structure. Computer technology has empowered individuals as never before. One study on enrolled student cybercrime suspects, for example, suggests that 77 per cent acted alone, rather than in a group.[109] One responding country in Western Asia also reported that most cybercrime acts were '*of an individual nature carried out by people for personal purposes and not in the form of organizations or groups.*'

As noted above, such conclusions may be heavily dependent upon conceptions of 'cybercrime' applied, and the nature of cases that come to the attention of national authorities.

---

103 BAE Systems Detica and London Metropolitan University, 2012. *Organised Crime in the Digital Age.*

104 Moore, T., Clayton, R., Anderson, R., 2009. The economics of online crime. *Journal of Economic perspectives*, 32(3):3-4.

105 BAE Systems Detica and London Metropolitan University, 2012. *Organised Crime in the Digital Age.*

106 *Norton Cybercrime Report. 2011.* Available at: http://us.norton.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf

107 UNODC, 2012. *Digest of Organized Crime Cases: A compilation of cases with commentaries and lessons learned.*

108 Study cybercrime questionnaire. Q85.

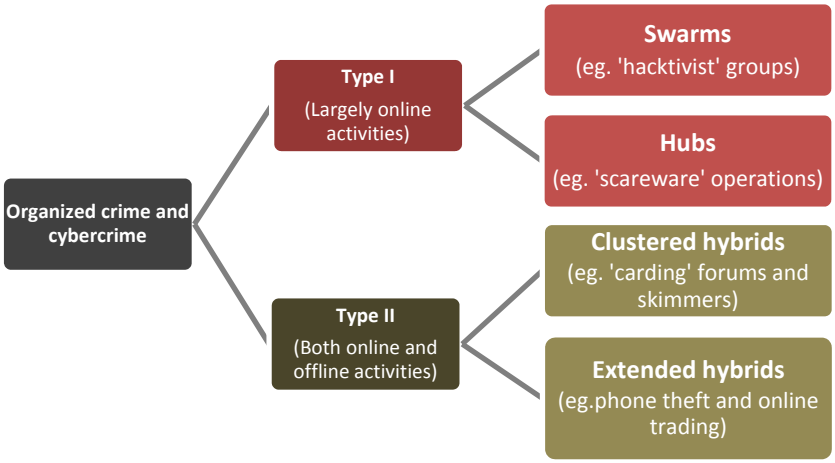
109 Lu, C.C., Jen, W.Y., Chang, W. and Chou, S., 2006. Cybercrime & Cybercriminals. *Journal of Computers*, 1(6):11-18. The study also finds that 63 per cent of all cybercrime suspects acted independently. It notes, however, that complicity is difficult to detect and it is likely that some cases of cybercrime identified as being independently perpetrated may actually be group perpetrated.

Overall, while criminal groups likely predominate in certain forms of cybercrime, it is clear that all typologies – including individual perpetrators – must be taken into account. The case examples contained in boxes in this Chapter, for example, demonstrate something of the range of perpetrator and group characteristics.

Group structure – One recent analysis of organized crime and cybercrime proposes a typology based on the degree of involvement of groups in online (as opposed to offline) activities and the structure of associations within the group.[110] Type I groups are suggested to have activities largely centred upon or directed at digital environments. Type II groups are proposed to have activities which switch between and across on and offline settings. Type I are further divided as 'swarms' (online-centric, dissociated structures) and 'hubs' (online-centric, associated structures).

From a law enforcement perspective, the de-centred, cellular nature of 'swarms,' with no obvious chain of command, may present policing difficulties. On the other hand, the fact that swarms are often amateur, with weaker checks on 'membership,' may represent policing opportunities. In contrast, 'hubs' can be more difficult to penetrate, but possess a clear command structure and key operatives on which law enforcement efforts can focus. Type II clustered and extended hybrids may have confusing, multiple-link-based structures that can only be targeted through individual law enforcement operations. The fact that such groups may be co-ordinated in some degree, however, presents opportunities for sequential action against (otherwise) individual criminal operations.[111] In addition, a proposed 'Type III' group perpetrates activities that are predominantly offline but increasingly intersect or are mediated through digital environments.[112] Evidence suggests that – while organizational structures often cross-cut in highly fluid ways – all of these group structures play a role in cybercrime offending. Hubs and clustered extended hybrids likely account for over 60 per cent of structures.[113]

Figure 2.15: Structures of organized criminal groups engaged in cybercrime



Source: BAE Detica/LMU

Organized crime and cybercrime markets – Organizational structures for financial-driven cybercrime, such as theft of banking details and credit card numbers, have been subject to particular analysis. A cybercrime 'black market' has been characterized in which groups and individuals with different roles and sometimes acting in multiple roles (including 'programmers', 'distributers', 'technical experts', 'hackers', 'fraudsters', 'hosters', 'cashers', 'money mules', 'tellers' and 'leaders')[114] interact in the process of malware creation, computer infection (such as through phishing emails),

110 BAE Systems Detica and London Metropolitan University, 2012. *Organised Crime in the Digital Age.*
111 *Ibid.* p.51.
112 *Ibid.* p.52.
113 *Ibid.* p.60.
114 See http://www.fbi.gov/news/speeches/the-cyber-threat-whos-doing-what-to-whom

botnet management, harvesting of personal and financial data, data sale, and 'cashing-out' of financial information.[115]

One mode of association within this market is the use of underground forums (often facilitated by anonymity services or 'onion routing' such as Tor) for the exchange of information and mediating the sale of consulting services, infection/spreading services, botnet rental, spam services, hosting, e-mail lists, and financial details.[116] While such markets can involve a large number of total individuals, associations may be transient – particularly in the case of money mules and criminal 'business' transactions, such as botnet rental from one individual or group to another. Botnets are used to commit attacks against information systems and to steal data, and are offered at relatively low cost, benefiting from the turnover based on the number of 'customers.' For example, a server with stored malware, exploit kits or botnet components costs anywhere from $80 to $200 a month. One botnet administration pack, known as the Eleonore Exploit Pack, has a retail value of $1,000. Renting a botnet of between 10 and 20 computers, administered using this pack, costs an average of $40 a day. A Zeus kit v1.3 costs $3,000 to $4,000.[117] These costs are relatively low compared to the potential financial gain, which may amount to anywhere from tens of thousands to tens of millions of dollars.

Perpetrator interactions

Complaints issued by law enforcement authorities in a country in North America in the course of criminal proceedings against a group of alleged transnational cybercrime perpetrators reveals the nature of perpetrator interactions within cybercrime markets. The extract below is from instant messages, or 'chats' obtained pursuant to a series of search warrants:

11:55:42:68 PM CC-4	how much your Trojan will cost me?
11:56:33:00 PM Alias-1	2k a month including hosting and support
…	
11:56:55:38 PM Alias-1	you can give it [meaning access to the botnet] to different people, checker and co-workers
…	
12:28:22:32 AM Alias-1	…I have .exe which gives at least 200-300 bucks from 1k of downloads for [different countries] [meaning [the botnet] will provide 200USD-300USD in stolen proceeds for every 1000 sets of stolen information from victims in [different countries]]

Source: http://www.justice.gov/usao/nys/pressreleases/January13/GoziVirusDocuments/Kuzmin,%20Nikita%20Complaint.pdf

The market as a whole is not a single criminal group enterprise. Rather, it can be characterized as a 'social network of individuals engaged in organized criminal activity.'[118] Certain individuals and small groups – such as the original programmers of malware, and botnet C&C owners – may represent key points within the market, around which other individuals, swarms, and hubs turn. Based on law enforcement investigations and arrests to date, those responsible for creating and managing key components of the market, such as botnets, appear to act in comparatively small groups, or even individually.[119] Out of a cohort of groups[120] identified and

115 See, for example, Fortinet, 2013. *Fortinet 2013 Cybercrime Report*; Panda Security, 2010. The *Cybercrime Black Market: Uncovered*; and Group IB, 2011. *State and Trends of the Russian Digital Crime Market.*

116 See, for example, Motoyama, M. *et al.*, 2011. *An Analysis of Underground Forums.* IMC 2011, 2-4 November 2011, Berlin; and Stone-Gross, B. *et al.*, 2011. *The Underground Economy of Spam: A Botmaster's Perspective of Coordinating Large-Scale Spam Campaigns.*

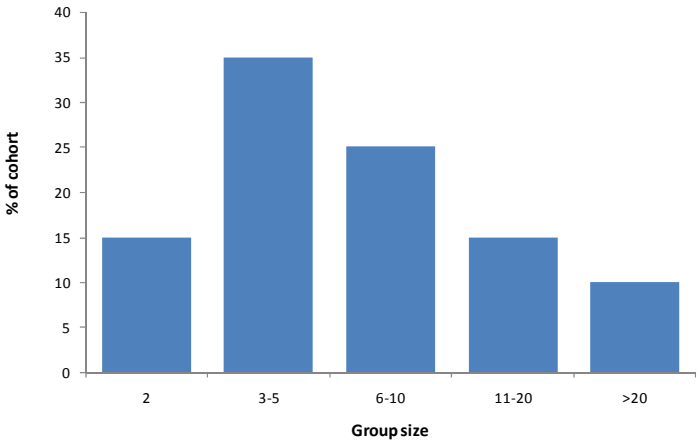
117 ESET Latin America's Lab, 2010. *ESET, Trends for 2011: Botnets and Dynamic Malware.* Available at: http://go.eset.com/us/resources/white-papers/Trends-for-2011.pdf

118 See, for example, Spapens, T., 2010. Macro Networks, Collectives, and Business Processes: An Integrated Approach to Organized Crime. *European Journal of Crime, Criminal Law and Criminal Justice*, 18:285-215.

119 See, for example, Bredolab botnet creator (http://nakedsecurity.sophos.com/2012/05/23/bredolab-jail-botnet/); Kelihos botnet creator (http://nakedsecurity.sophos.com/2012/01/24/microsoft-kelihos-botnet-suspect/); Mariposa botnet creator (http://nakedsecurity.sophos.com/2012/08/07/mariposa-botnet-trial/); and SpyEye convictions (http://nakedsecurity.sophos.com/2012/07/01/uk-cops-announce-sentencing-of-baltic-malware-trio/)

reviewed by the BAE Detica/LMU study, for example, the most common organizational pattern was found to be associations of 3-5 individuals who had operated together for around a year.[121] Half of the groups comprised 6 or more individuals, with one quarter comprising 11 or more. One-quarter of active groups had operated for less than six months. However, group size or the length of association does not necessarily correlate with the impact of offending – small groups can inflict large damage within a short time.

Figure 2.16: Typical sizes of organized criminal groups engaged in cybercrime



Source: BAE Detica/LMU

Where individuals and associations within the market do not themselves meet the formal organized crime definition, it is nonetheless possible that they may fall within the association or conspiracy provisions of Article 5 of the Organized Crime Convention that cover conspiracy and/or criminal association types of offences, as well as organizing, directing, aiding, abetting, facilitating or counselling the commission of a serious crime involving an organized criminal group.[122]

Geographical distribution – While it is often assumed that cybercriminals operate in a decentralized, global manner, evidence suggests that groups may still be located in close geographical proximity, even if their activities are transnational. For example, local and regional networks, in addition to close networks of family and friends, remain significant factors. Indeed, even where groups associate largely through online contact, there is evidence that they use methods of association and forms of knowledge which have 'local' characteristics. This gives rise to a 'glocalizing' effect in which linguistic and cultural factors are used by organized criminal groups to further their activity. Many underground online forums, for instance, are

'ZeuS Malware'

Software engineers in Eastern Europe have used malware known as the 'ZeuS' virus. Target computers are compromised once the victim opens an apparently benign e-mail message. With access to the victim's bank account numbers and password details, perpetrators are able to log on to the victim's bank accounts. Accomplices of the principals placed notices on Russian language websites inviting students resident in North America to assist in transferring funds out of the country. These so-called 'mules' were provided with counterfeit passports and directed to open accounts in false names in various North American financial institutions. When principals transferred funds from legitimate account holders to the mules' accounts, the mules were instructed to move the funds to accounts offshore, or, in some cases, to smuggle the funds physically out of North America. Five individuals were arrested in Eastern Europe, 11 in Northern Europe and 37 charged in North America. The motive of participants appears to have been primarily financial. The repetitive nature and volume of individual offences attracted the attention of the authorities and contributed to the interdiction of the conspiracy.

http://www.justice.gov/usao/nys/pressreleases/September10/operationachingmulespr%20FINAL.pdf

120 It should be noted that the BAE Systems and London Metropolitan University study includes groups of 2 persons. These associations fall outside of the definition contained in Article 2(a) of the Organized Crime Convention, which refers to a group of 3 or more persons.

121 BAE Systems Detica and London Metropolitan University, 2012. *Organised Crime in the Digital Age.*

122 See Organized Crime Convention, Arts. 5(1)(a) and (b).

characterized by the use of local languages, nicknames, and cultural markers. This has the effect both of making it difficult for law enforcement to penetrate, and of self-identifying trusted criminal associates.

Locations showing a high level of cybercrime activity with potential links to organized crime are found, amongst others, in countries in Eastern Europe and Eastern Asia. The ZeuS malware, for example, originated in Eastern Europe in 2007, and notable hubs for cybercrime have also been reported elsewhere in Eastern Europe.[123] Interestingly, this pattern matches well with data showing the location of botnet command and control servers presented in this Chapter.[124] There is also increasing concern about the scale of cyber-victimization in Eastern Asia, including a possible significant role for domestic crime groups.[125]

123 Bhattacharjee, Y., 2011. Why Does A Remote Town In Romania Have So Many Cybercriminals? *Wired*, 19(2):82.

124 See above, Section 2.2 The global cybercrime picture, Criminal tools – the botnet.

125 Kshetri, N., 2013. *Cybercrime and Cybersecurity in the Global South*. Houndmills, UK: Palgrave Macmillan, Chapter 3; Broadhurst, R., Chang, Y.C., 2013. Cybercrime in Asia: trends and challenges. *In:* Hebenton, B., Shou, S.Y. and Liu, J. (eds.) *Asian Handbook of Criminology*. Springer.

Page left intentionally blank

CHAPTER THREE: LEGISLATION AND FRAMEWORKS

This Chapter examines the role of national, international and regional legislation and frameworks in the prevention and combating of cybercrime. It finds that legislation is required in all areas, including criminalization, procedural powers, jurisdiction, and international cooperation. While the last decade has seen significant developments in the promulgation of multilateral instruments aimed at countering cybercrime, the Chapter highlights a growing legal fragmentation at international and national level.

3.1 Introduction – The role of law

Key results:

- The technological developments associated with cybercrime mean that – while traditional laws can be applied to some extent – legislation must also grapple with new concepts and objects, such as intangible 'computer data,' not traditionally addressed by law
- Legal measures are crucial to the prevention and combating of cybercrime, and are required in all areas, covering criminalization, procedural powers, jurisdiction, international cooperation, and internet service provider responsibility and liability
- At the national level, cybercrime laws most often concern criminalization – establishing specialized offences for core cybercrime acts. Countries increasingly recognize the need, however, for legislation in other areas
- Compared to existing laws, new or planned cybercrime laws more frequently address investigative measures, jurisdiction, electronic evidence and international cooperation

Cyber-specificity

Legal measures play a key role in the prevention and combating of cybercrime. Law is dynamic tool that enables the state to respond to new societal and security challenges, such as the appropriate balance between privacy and crime control, or the extent of liability of corporations that provide services. In addition to national laws, at the international level, the *law of nations* – international law – covers relations between states in all their myriad forms. Provisions in both national laws and international law are relevant to cybercrime.

The technological developments associated with cybercrime mean that – while traditional laws can be applied to some extent – legislation must also grapple with new concepts and objects, not traditionally addressed by law. In many states, laws on technical developments date back to the 19th century. These laws were, and to a great extent, still are, focused on *physical* objects – around which the daily life of industrial society revolved. For this reason, many traditional general laws do not take into account the particularities of information and information technology that are associated with cybercrime and crimes generating electronic evidence. These acts are largely characterized by new *intangible* objects, such as data or information.

While *physical objects* can usually be attributed exclusively to certain owners, attribution of *information* ownership can be significantly more challenging. This difference is relevant, for example, to the legal concept of 'theft', applied in the traditional laws of many countries. A 'theft' of computer data, for instance – even given the extension of the concept of objects to include data or information – may not fall within the scope of the constituent elements of traditional theft. The data would still remain in the possession of the original bearer, thus (depending upon national law approaches) possibly not meeting required legal elements, such as 'expropriation' or 'taking' of the object. Similarly, legal references to a public or private 'place' in harassment or stalking laws may, or may not (again, depending upon national approaches) extend to online 'places.' Such examples illustrate a potential need – in some areas – for the adaptation of legal doctrines to new information technologies.[1]

Functions of cybercrime legislation

- Setting clear standards of behaviour for the use of computer devices
- Deterring perpetrators and protecting citizens
- Enabling law enforcement investigations while protecting individual privacy
- Providing fair and effective criminal justice procedures
- Requiring minimum protection standards in areas such as data handling and retention
- Enabling cooperation between countries in criminal matters involving cybercrime and electronic evidence

This raises the question of whether cybercrime should be covered by general, existing criminal law provisions, or whether new, computer-specific offences are required. The question cannot be answered generally, but rather depends upon the nature of individual acts, and the scope and interpretation of national laws. Chapter Four (Criminalization) of this Study examines the use of specialized, and general, laws in the criminalization of cybercrime acts. Country responses show that some 'core' cybercrime offences are covered by cyber-specific offences, while others are covered by general offences.[2] Chapters Five (Law enforcement and investigations) and Eight (Prevention) consider the use of information-specific or cyber-specific laws that may be required in areas such as law enforcement investigative powers[3] and the liability of internet service providers.[4]

Relevant categories of law

While *criminal* law is often perceived as being most relevant when it comes to cybercrime, possible legal responses also include the use of *civil* law (which addresses the legal relationship between persons), and *administrative* law (which addresses the legal relationship between persons and the state). Further divisions within these legal regimes include *substantive* and *procedural* law, as well as *regulatory* and *constitutional*, or *rights-based*, laws. In many legal systems, each of these regimes are characterized by specific aims, institutions, and safeguards. Cybercrime laws are most usually found within the areas of substantive and procedural criminal law. However, a number of other areas of law are also important.

In particular, the range of computer-related acts that the state may wish to regulate will not always require the use of intrusive criminal law measures. Computer-related acts that are considered minor infringements, for example, may be addressed by civil and administrative regulations, rather

1 Sieber, U., 2012. Straftaten und Strafverfolgung im Internet. *In*: *Gutachten des Deutschen Juristentags*, Munich: C.H. Beck, pp.C 14-15.

2 See Chapter Four (Criminalization), Section 4.1 Criminalization overview, Cyber-specific and general offences.

3 Existing studies propose that computer-specific provisions are required in investigative powers in order to permit actions such as expedited preservation of data and the use of remote forensics tools; see Sieber, U., 2012. Straftaten und Strafverfolgung im Internet, *In: Gutachten des Deutschen Juristentags*. Munich: C.H. Beck, pp.C 62-72, 103-128.

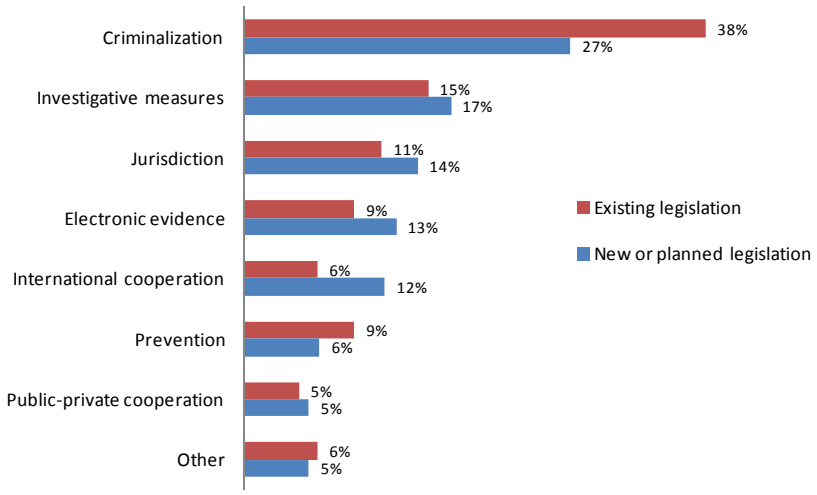
4 The transmission or hosting of large volumes of third-party content by internet service providers, for example, renders impracticable the application of traditional liability rules applicable to the press and media – who are often obliged to control content prior to publication. Rather, general liability is replaced by specific conditions, including 'notice' and 'take-down' procedures. See Chapter Eight (Prevention), Section 8.3 Cybercrime prevention, the private sector, and academia, Cybercrime prevention by internet service and hosting providers.

than by criminal legislation. In addition, criminal statutes often refer to underlying civil and administrative law standards, such as in the areas of copyright law or data protection law. Combined provisions can also provide for criminal, administrative and civil liability at the same time. Thus, legislation relevant to cybercrime may address a wide range of issues, including: criminalization of particular conduct; police investigative powers; issues of criminal jurisdiction; admissibility of electronic evidence; data protection responsibilities of electronic service providers; and mechanisms of international cooperation in criminal matters involving cybercrime.

This breadth of areas was reflected by responding countries. When asked to report legislation relevant to cybercrime, countries referred to a number of laws, including: criminal codes; laws on high-tech crime; criminal procedural codes; laws on wiretapping; evidence acts; laws on electronic communications; laws on security of information technologies; laws on personal data and information protection; laws on electronic transactions; cybersecurity acts; and laws on international cooperation.[5]

Figure 3.1 shows the areas covered by legislation reported by countries through the Study questionnaire. The data represents the distribution of over 250 reported existing, and over 100 new or planned pieces of legislation.[6] Criminalization is the predominant area of focus for both existing, and new or planned legislation. As discussed in Chapter Four (Criminalization), this includes both cyber-specific and general criminal provisions. The fact that criminalization represents the most frequent area for new or planned legislation indicates a continued focus of countries on the development of new cyber-specific offences, and/or the adaptation or amendment of existing general offences.

Figure 3.1: Cybercrime legislation areas



Source: Study cybercrime questionnaire. Q12 and Q14. (n=55,36; r=262,111)

A clear pattern, however, is a reduction in the relative proportion of new or planned legislation (compared to *existing* legislation) that concerns criminalization, and an increase in relative attention to other areas, such as investigative measures, jurisdiction, electronic evidence, and, notably, international cooperation. This may indicate a trend – at least amongst responding countries – towards increasing recognition of the need for cybercrime legislation across a spectrum of legislative areas.

By way of introduction to these legislative areas, this section briefly introduces relevant legal considerations for each.

Criminalization - The principle of *nullum crimen sine lege* (no crime without law) requires that the conduct constituting any criminal offence must be described clearly by law.[7] As discussed above,

5 Study cybercrime questionnaire. Q12.
6 Legislation reported in response to Study cybercrime questionnaire. Q12 and 14.
7 While, in common law countries, judicial competencies for developing and extending criminal law have traditionally been greater, modern approaches to criminalization require statute-based law even in core common law systems. See *U.S. v. Hudson and Goodwin*,

in order to unambiguously describe cybercrime conduct, criminal laws may require the introduction of new 'information-related' legal objects, as well as extended protection of traditional legal interests against new forms of computer-related acts. New objects required may include definitions such as 'computer data' or 'computer information', and legal interests such as the 'integrity' of computer systems.

Through such concepts, the criminal law has the tools to protect against violation of the 'cyber'-interests that persons have – for example, in controlling access to a computer system that they own. Different legal systems have different basic criteria for identifying conduct that may legitimately be the object of criminal law.[8] The systematic application of these criteria to cyber-related conduct can be challenging. Nonetheless, in many national systems, and in some international or regional initiatives, there is evidence of theoretical work that aims to underpin the criminalization of cyber-conduct. The Explanatory Report to the Council of Europe Cybercrime Convention, for example, refers extensively to 'legal interests' and the 'harms' at stake.[9] Where a strong justification for the criminalization of a particular conduct does not exist, a risk of *over*-criminalization arises. In this respect, international human rights law represents one important tool for the assessment of criminal laws against an external, international standard. Chapter Four (Criminalization) of this Study examines further a number of common cybercrime offences and their construction both in national and international law.

In addition to the specific conduct criminalized, any study of cybercrime offences must take into account the *general part* of criminal law. This is the part that deals with issues applicable to all offences, such as complicity, attempt, omission, state of mind (intent), defences, and criminal liability of legal persons. Cybercrime offences are, in general, subject to the general part of criminal law in the same way as for any other specific offence. Many responding countries indicated, for example, that 'generally' criminal offences are limited to intentional acts.[10] Nonetheless, such general positions can be amended for particular acts – such as where a 'specific intent' is required. Chapter Four (Criminalization) examines this issue in greater depth.

Procedural powers – An effective investigation of crime is not possible without adequate investigative powers. Due to their often intrusive nature, such measures must be regulated by law and accompanied by adequate safeguards. While some investigative actions can be achieved with traditional powers, many procedural provisions do not translate well from a spatial, object-oriented approach to one involving electronic data storage and real-time data flows. Specialized powers are therefore required, such as for the gathering of electronically stored and communicated computer content, for the identification and localisation of computer devices and communications, for the quick 'freeze' of volatile computer data, and for 'undercover' online investigations.[11] Such powers are not only required for the investigation of 'cybercrime' itself, but also for the investigation of any crime generating electronic evidence. Chapter Five (Law enforcement and investigations) examines a number of specialized investigatory powers found in national and international laws.

Gathering and using evidence – Traditional criminal procedural law typically contains provisions on the gathering and admissibility of evidence. When it comes to evidence in electronic form,

---

11 U.S. 32 (1812); Dubber, M., 1999. Reforming American Penal Law. *Journal of American Criminal Law and Criminology,* 90(1)49-114; and Simester, A.P., Spencer, J.R., Sullivan, G.R., Virgo, G.J., 2010. *Criminal Law.* 4th ed. Oxford/Portland: Hart Publishing, p.46.

8 Including concepts such as harm, offense, wrongfulness, morality, paternalism, legal goods and deterrence. See Ashworth, A., 2006. *Principles of Criminal Law*. 6th ed. Oxford: Oxford University Press, p.27; Dubber, H., 2005. Positive Generalprävention und Rechtsgutstheorie. *Zeitschrift für die gesamte Strafrechtswissenschaft,* pp. 485-518, pp.504 et seq.; Hassemer, W., 1980. *Theorie und Soziologie des Verbrechens.* Frankfurt a.M.; Feinberg, J. 1984. *Harm to Others.* Oxford: Oxford University Press.

9 Council of Europe. 2001. *Explanatory Report to the Convention on Cybercrime.*

10 Study cybercrime questionnaire. Q40.

11 Sieber, U., 2012. Straftaten und Strafverfolgung im Internet. *In: Gutachten des Deutschen Juristentags.* Munich: C.H. Beck, pp.C14-15.

computer data can be altered easily. Thus, the gathering and handling of electronic evidence must guarantee the integrity, authenticity and continuity of evidence during the entire time period between its seizure and its use in trial – a process often known as the 'chain of custody.' Country responses to the study questionnaire highlight that while some countries create special evidential rules for electronic evidence, others prefer to treat it in the same way as all other forms of evidence. In jury-based common law countries, laws may deal more extensively with evidence and admissibility rules, whereas continental law countries often rely on the principle of free judicial evaluation of evidence.[12] Chapter Six (Electronic evidence and criminal justice) examines the issue of electronic evidence in greater depth.

Regulation and risk – Criminal law focuses on bringing offenders responsible for *past* acts to justice. Regulatory and risk reduction or anticipation laws, on the other hand, aim at reducing the risk that *future* acts will occur, or at making it easier for law enforcement authorities to carry out law enforcement investigations and criminal justice actions should acts occur.[13] With respect to cybercrime, a number of approaches, including internet filtering, data protection, data retention, and pro-active actions against criminal infrastructure fall within this category. The 'anticipatory' nature of laws authorizing many of these actions requires that they be accompanied by particular safeguards, in order to ensure that they do not represent disproportionate infringements of individual rights, or unnecessarily involve the use of coercive powers.[14] Chapter Eight (Prevention) examines, amongst other prevention aspects, a number of such regulatory frameworks.

Jurisdiction and international cooperation – More than half of responding countries reported that between 50 and 100 per cent of cybercrime acts encountered by police involved a 'transnational element.'[15] The prosecution of transnational acts requires states to assert two types of 'jurisdiction' – both substantive and investigative. Firstly, states must be able to assert that their national criminal law applies to an act that takes place only partly, or even not at all, within its national territory. Secondly, states need to be able to carry out investigative actions that concern the territory of other states. In so far as investigations may involve infringements on the sovereignty of states, formal and informal processes of consent and international cooperation are required. Many of these are at the level of international treaty law, both multilateral and bilateral. National laws, however, can also specify procedures to be applied, or create bases for cooperation in their own right. Chapter Seven (International cooperation) examines this area in detail.

---

12 Damaska, M.R., 1973. Evidentiary Barriers to Conviction and Two Models of Criminal Procedure: A Comparative Study. *University of Pennsylvania Law Review* 121(3):506-589 (1972-73).

13 Sieber, U., 2012. Straftaten und Strafverfolgung im Internet. *In*: *Gutachten des Deutschen Juristentags*. Munich: C.H. Beck, note **1**, pp.C 69-74.

14 See European Commission. 2012. *Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century*, COM(2012) 9 final. Available at: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_9_en.pdf

15 Study cybercrime questionnaire. Q83.

3.2 Divergence and harmonization of laws

Key results:

- Harmonization of cybercrime laws is essential for, *inter alia*, the elimination of criminal safe havens, and global evidence collection
- Divergences in national cybercrime laws derive from a range of factors, including underlying legal and constitutional differences
- The area of cybercrime offence penalties well exemplifies divergences in national approaches to cybercrime acts. Examination of just one crime – illegal access – shows considerable difference in its perceived degree of seriousness
- One-third of responding countries report that their legislation is highly, or very highly harmonized with countries viewed as important for the purposes of international cooperation
- This varies regionally, however, with higher degrees of harmonization reported by countries in the Americas and Europe
- This may be due to the use, in some regions, of multilateral instruments, which are inherently designed to play a role in harmonization

Underlying differences in laws

In today's globalized world, the law consists of a multitude of national, regional and international legal systems. Interactions between these systems occur at multiple levels. As a result, provisions sometimes contradict each other, leading to collisions of law, or fail to overlap sufficiently, leaving jurisdictional gaps.[16]

Criminalization differences – Case example

A citizen of a country in Oceania uploaded legal material containing forms of hate speech on a server in his own country. The material was downloaded in a European country. When the individual later travelled to that country in Europe, he was arrested and sentenced to imprisonment for these acts, which had not been criminal in his home country.

The case was appealed. The Federal High Court of the European country upheld the conviction. It argued that although the accused neither acted in the European country nor actively sent his data to this country, he nonetheless threatened the public peace within the territory, as required by the relevant statute The court stressed, however, that the interpretation could not be generalized for other statutes on illegal content.

Source: Judgement of the German Bundesgerichtshof of 1 December 2000 (1 StR 184/00, please see BGH MMR 2001, pp.228 et seqq.)

Cybercrime is by no means the first 'new' form of crime to engage multiple jurisdictions and laws. Illicit trafficking flows in drugs, people and weapons, for example, frequently originate and end in different hemispheres, passing through many countries in between. Nonetheless, cybercrime acts can engage legal jurisdictions within the timeframe of milliseconds. Computer content, for example, can be legally stored on a computer server in one country, but downloaded through the internet in multiple countries, some of which may consider the content to be illegal.[17]

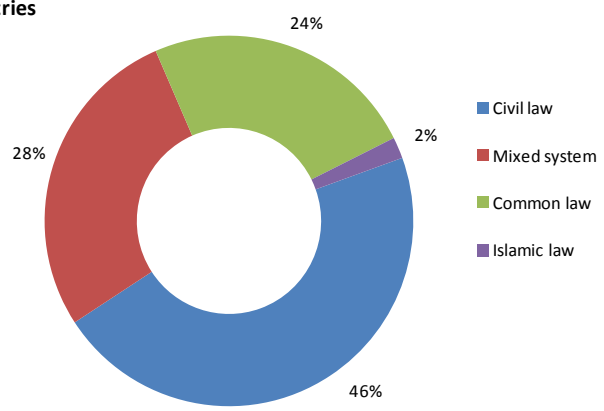
16 Sieber, U., 2010. Legal Order in a Global World. *In*: Von Bogdandy, A., Wolfrum, R. (eds.) *Max Planck Yearbook of United Nations Law*, 14:1-49.

17 Sieber, U., 2008. Mastering Complexity in the Global Cyberspace. *In*: Delmas-Marty, M., Pieth, M., and Sieber, U. (eds.) *Les chemins de l'harmonization pénale*. Paris, pp.127-202 (192-197).

Differing global perspectives on the acceptability of forms of internet content leave a number of theoretical alternatives. States could choose to restrict the scope of their criminal jurisdiction to activities of perpetrators on their own national territory. They could focus on the prosecution of persons within their territory accessing content, irrespective of its source. Or they could attempt extraterritorial action against content producers. Such perspectives illustrate the growing extent of legal differences and approaches in the area of cybercrime. Chapter Four (Criminalization) examines this point in greater depth, including from the perspective of international human rights law.

Some divergences between national laws can be traced back to fundamental differences between *legal families*. Major legal families commonly identified include continental European law,[18] common law,[19] Islamic law,[20] and mixed law (such as Chinese law).[21] Country responses to the Study questionnaire show that a broad range of legal systems are represented.[22]

Figure 3.2: Classification of national legal system of responding countries



Study cybercrime questionnaire. Q15. (n=54)

Legal families are an important way of characterizing legal heritage, including where systems share particular features, due for instance to common cultural roots.[23] Nonetheless, national laws are not static, and similarities between systems may exist at a certain point in time, but subsequently vanish.[24] As such, historic differences can disappear or lose their practical relevance.

18 Continental European criminal law is often characterized by abstract normative rules, systematic structures and a strong influence of academic thinking. Criminal law is usually extensively codified with penal codes also providing for general principles of criminal responsibility applicable to all forms of criminal behaviour. See Zweigert, K., Kötz, H. 1998. *Comparative Law*. 3rd ed. Oxford/New York: Clarendon Press, p.69. See also Weigend, T. 2011. *In*: Heller, K.J., Dubber, M.D. (eds.) *The Handbook of Comparative Criminal Law*, Stanford: Stanford University Press, pp.256 et seq.; Elliott, C., *ibid*., p.213.; Gómez-Jara Díez, C., Chiesa, L.E., *ibid*., p.493; Thaman, S.C., *ibid*., p.416.

19 In contrast, in common law jurisdictions, substantive laws provisions are more usually drafted in descriptive terms, ensuring both accessibility of law, and reflecting the strong position of lay judges within common law jurisdictions. Judge-made law was long the main source of the substantive criminal law and still remains an important element. Codification, however, is now a widespread norm, albeit sometimes through separate legislative acts rather than one single penal code. See Legeais, R., 2004. *Grands systèmes de droit contemporains*. Paris: Litec, pp.357, 366; Ashworth, A. (United Kingdom). 2011, p.533, and also Robinson, P. (United States) 2011, p.564. Both *in*: Heller, K.J., Dubber, M.D. (eds.) *The Handbook of Comparative Criminal Law*, Stanford: Stanford University Press; Simester, A.P., Spencer, J.R., Sullivan, G.R., Virgo, G.J. 2010. *Criminal Law*. 4th ed. Oxford/Portland: Hart Publishing, p.46; Ashworth, A. 2009. *Principles of Criminal Law*. 6th ed. Oxford/New York: Oxford University Press, p.8.

20 Islamic law is characterized by Shari'a, the sacred law of Islam, and fiqh, the jurisprudence of Islamic jurists. Crimes are categorized according to their legal sources and to punishments provided. A number of core offences are sanctioned by the use of fixed penalties (hudud). Other core offences are punished through legal reasoning based on Ijma and Qiyas. In general, Islamic laws allow for extensive flexibility as regards criminalization, including through the evolution of different theological schools of law. See Tellenbach, S., 2011. *In*: Heller, K.J., Dubber, M.D. (eds.) *The Handbook of Comparative Criminal Law*. Stanford: Stanford University Press, p.321.

21 Chinese criminal law has been influenced by a range of legal systems with the judiciary retaining important powers to give binding judicial interpretations of law. See Luo, W., 2011. *In:* Heller, K.J., Dubber, M.D. (eds.) *The Handbook of Comparative Criminal Law.* Stanford: Stanford University Press, p.138; and Bu, Y., 2009. *Einführung in das Recht Chinas.* Munich: C.H. Beck, p. 20.

22 Study cybercrime questionnaire. Q15.

23 See Ferrante, M., 2011. *In:* Heller, K.J., Dubber, M.D. (eds.) *The Handbook of Comparative Criminal Law*. Stanford: Stanford University Press, p.13.

24 Zweigert, K., Kötz, H. 1998. *Comparative Law*. 3rd ed. Oxford/New York: Clarendon Press, p.66.

When it comes to cybercrime, some remaining historical legal differences in national criminal procedure law certainly persist.[25] Nonetheless, differences in the overall content of the criminal law often depend less on the particular 'legal family' – be it civil or common law – and more on prevailing socio-cultural and constitutional orders. The placement of varying emphasis, for example, on values such as freedom of expression and privacy, or on the individual or community, can have a significant influence on policy and criminalization outcomes. In the context of cybercrime, this can lead to different legal results in areas such as regulation of obscene material;[26] balances between freedom of speech and unacceptable expression;[27] levels of access to internet content;[28] rules and obligations for internet service providers;[29] and safeguards and limitations on intrusive law enforcement investigations.[30]

In addition to socio-cultural and constitutional effects, the impact on legal drafting processes of simple historical coincidences, the impact of views of individual experts, and differing evaluations of best practice, should not be underestimated. Technical legal differences that arise from such effects, as well as from legal procedural heritages, may be significantly more straightforward to account for and to address, than those that derive from socio-cultural and constitutional orders.

Harmonization of laws

Such differences lead to the question of whether, and if so, how far, national legal differences in cybercrime laws can and should be reduced. In other words, how important is it to harmonize cybercrime laws? This can be undertaken in a number of ways, including through both binding and non-binding international or regional initiatives. The basis of harmonization may be a single national approach (with all others revising their laws in line), or, more often, common legal elements identified in the law of a number of states, or expressed within a multilateral instrument – such as a treaty or non-binding international standard. Indeed, as discussed further below, one of the aims of international law is to achieve harmonization of national laws.

During information gathering for the Study, countries were asked about perceived degrees of harmonization of cybercrime legislation, and about successes and limitations of harmonization, and approaches used to maintain national legal traditions during harmonization processes.[31] A number of countries, in Asia and the Americas in particular, highlighted that while harmonization was important, the process was subject to some important limitations. These included '*conflict… with constitutional requirements,*' requirements that harmonization should not be '*in conflict with Basic Law and Sharia*', needs for '*contextual application*' of harmonized standards, and issues of the existence of both federal and state legislation within a country.[32] Countries also reported successes in harmonization of cybercrime legislation. Countries highlighted, for example, that harmonization was part of a '*comprehensive approach to include substantive and procedural rules of law*', and that national legal traditions

---

25 On the evolving and heterogeneous nature of procedural law, see Legeais, R., 2004. *Grands systèmes de droit contemporains*. Paris: Litec, p.389.

26 See, for instance, Segura-Serrano, A., 2006. Internet Regulation and the Role of International Law. *In*: Von Bogdandy, A., Wolfrum, R. (eds.) *Max Planck Yearbook of United Nations Law*, 10(2006):191-272; Edick, D.A. 1998. Regulation of Pornography on the Internet in the United States and the United Kingdom: A Comparative Analysis. *Boston College International & Comparative. Law Review* 21(2):437-460.

27 See *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. A/67/357, 7 September 2012.

28 *Ibid.*

29 See *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. A/HRC/17/27, 16 May 2011.

30 For instance, regarding investigations into computer-related acts in support of terrorism offences, see UNODC. 2012. *The use of the Internet for terrorist purposes*. paras 35, 106, 110.

31 Study cybercrime questionnaire. Q16 and Q17.

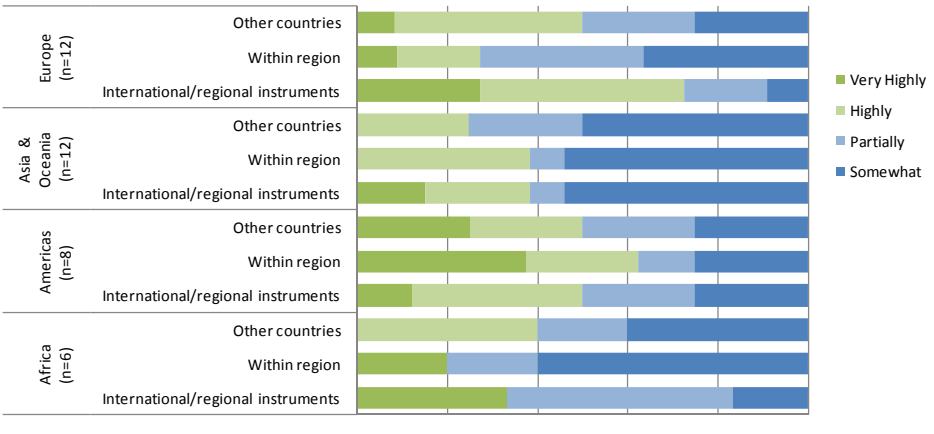
32 *Ibid.* Q16.

could still be maintained by '*taking into account the specificity of society in terms of customs, traditions and usages*… [and] *pre-existing national legislation.*'[33]

The degree of harmonization of cybercrime laws reported by responding countries varies significantly depending upon region, and upon whether harmonization was considered with respect to: (i) other countries; (ii) within the region; or (iii) the provisions of multilateral instruments. Overall, Figure 3.3 below shows that around one-third of countries reported that their legislation was either 'very highly' or 'highly' harmonized with other countries. The remainder view their legislation as 'partially' or 'somewhat' harmonized with other countries. Levels of perceived harmonization tend to be higher in Europe and the Americas, than in Africa, Asia and Oceania. One country in Asia, for example, commented directly that '*current legislation is not harmonized with countries that are important… for the purposes of international cooperation.*'[34] Other countries referred to the global situation. One country in Europe, for example, noted that '*at regional level there is a high degree of harmonization. At global level we are not aware if it is the same. Although no international judicial cooperation request was* [*yet*] *refused to us based on the lack of double criminality requirements, it is apparent that different procedural rules…* [*exist*] *related to international judicial cooperation.*'[35]

Many countries commented on the utility of international instruments in processes of harmonization. One country, for example, reported finding it useful to have external standards, such as those found in international and regional instruments, '*against which we could compare the provisions of our laws.*'[36] Another noted that international *fora* seeking consensus on international strategies and legal measures against cybercrime were important as they represented '*opportunities to share ideas which can be taken up by any Member State as useful legislative or practical options for preventing and suppressing crime.*' The same country observed that harmonization processes represented a two-way process, as '*in some cases… domestic legislative initiatives or ideas have been the source of elements in international norms, and it other cases, ideas expressed by other Member States have influenced* [*national*] *thinking about cybercrime, and have found their way into* [*national*] *law as a result.*'[37] Other countries noted the influence of existing national legislation. One country in Eastern Asia, for example, stated that it had '*studied foreign legislation…to establish national legislation.*'[38] Overall, Figure 3.3 is rather inconclusive as to the impact of international instruments on harmonization. High levels of perceived harmonization of national

Figure 3.3: Degree of harmonization of cybercrime legislation with: (i) other countries important for cooperation, (ii) the Region, and (iii) multilateral instruments



Source: Study cybercrime questionnaire. Q17. (n=38)

33 *Ibid.*
34 Study cybercrime questionnaire. Q17.
35 *Ibid.*
36 Study cybercrime questionnaire. Q16.
37 Study cybercrime questionnaire. Q17.
38 Study cybercrime questionnaire. Q16.

legislation with international instruments for countries in Europe, for example, do not appear to translate directly into high levels of harmonization with countries within the region.

International instruments relevant to cybercrime and their influence on national legislation are examined later in this Chapter. Firstly, however, it is important to examine the *reasons* and *rationale* behind harmonization of cybercrime legislation.

Why harmonize?

To avoid criminal safe havens – In the field of cybercrime, as for all transnational crimes, the main advantage of harmonizing criminal law lies in the prevention of cybercrime safe havens for perpetrators. As noted by one respondent country to the Study questionnaire, '*cybercrime is a global problem, and this makes all countries important to us, in one of several ways… we believe that cooperation with developing countries is important on the basis that cybercrime knows no boundaries.*'[39] Indeed, out of all transnational crimes, cybercrime likely offers the most direct risk for use of safe havens.

Thus, if harmful acts involving the internet are criminalized, for example, in State A, but not in State B, a perpetrator in State B can be free to target victims in State A via the internet. In such cases, State A cannot, on its own, effectively protect against effects from such transnational activities. Even where its criminal law allows the assertion of jurisdiction over the perpetrator in State B, it will still require consent or assistance from B – either regarding the gathering of evidence, or the extradition of the identified perpetrator. In order to protect persons within its own jurisdiction, State B is unlikely to assist where the conduct is not also criminalized in its own country. This principle of *dual criminality* is central to many forms of international cooperation. It can be found, for example, in multilateral and bilateral *extradition* treaties, as well as national laws.[40]

Dual criminality also plays a role in *mutual legal assistance*, such as requests for interviewing of witnesses, or collection of evidence.[41] While not all mutual legal assistance agreements between states include this requirement, many instruments ensure that coercive or intrusive measures, such as search and seizure, or freezing of property, are subject to dual criminality.[42] Chapter Seven (International cooperation) examines this area in greater detail. For the purposes of *harmonization* of cybercrime criminal laws, however, an important point is that dual criminality does not require that the underlying activity be punished by the same type of legal provision. Thus, if State C uses a cyber-specific offence for particular conduct, while State D uses a general offence, both C and D will be able to engage in international cooperation, provided that the essential constituent *elements* of the offence are comparable under the laws of both states.[43] As discussed in Chapter Seven, where states achieve a certain degree of harmonization among their national laws (such as in the European

---

39 Study cybercrime questionnaire. Q17.

40 See, for example, Article 2(1) of the United Nations Model Treaty on Extradition, Article 2(1) of the European Convention on Extradition, and Article 2 of The London Scheme for Extradition within the Commonwealth. See also Plachta, M., 1989. The role of double criminality in international cooperation in penal matters. *In*: Agell, A., Bomann, R., and Jareborg, N. (eds.) *Double criminality, Studies in international criminal law*. Uppsala: Iustus Förlag, p.111, referring to, *inter alia*, Shearer, I., 1971. *Extradition in international law*. Manchester, p. 137, and Bassiouni, M.C., 1974. *International extradition and world public order*. Dordrecht: Kluwer Academic Publishers, p.325.

41 See Capus, N., 2010. *Strafrecht und Souveränität: Das Erfordernis der beidseitigen Strafbarkeit in der internationalen Rechtshilfe in Strafsachen*. Bern: Nomos, p.406.

42 See, for example, Article 5(1) of the Council of Europe Convention on Mutual Legal Assistance, and Article 18(1)(f) of the Council of Europe Convention on Laundering, Search, Seizure, and Confiscation of the Proceeds from Crime. For the exchange of information or other forms of cooperation that do not infringe upon the rights of the person concerned, dual criminality has not been required. See Vermeulen, G., De Bondt, W., Ryckman, C., 2012. *Rethinking International Cooperation in Criminal Matters in the EU*. Antwerp: Maklu, p.133; and Klip, A., 2012. *European Criminal Law*. Antwerp: Intersentia, p.345.

43 Plachta, M., 1989. The role of double criminality in international cooperation in penal matters. *In*: Agell, A., Bomann, R., Jareborg, N. (eds.). *Double criminality, Studies in international criminal law*. Uppsala: Iustus Förlag, pp.108-109. See also: *Explanatory report to the European Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime,* that specifies in the clarification of Art. 18(1)(f) that dual criminality is required in abstract to for the investigative measures meant by Section 2, which includes (but is not limited to) the investigative measures that require coercive action.

Union), the principle of dual criminality may come to be replaced by a default presumption of equivalence of laws.[44]

To enable global evidence collection – The harmonization of procedural law is a second indispensable requirement for effective international cooperation. In the above example, if State B does not have the necessary procedural power for expedited preservation of computer data, for instance, then State A will not be able to request this facility through mutual legal assistance. In other words, a requested state can only provide assistance within its territory, to the extent that it could do so for an equivalent *national* investigation.[45] Again, as with dual criminality, the legal *form* of the procedural power need not be directly equivalent, as long as the investigative measure can be executed in practice. Securing expedited preservation of data, for example, might legitimately be achieved either through a dedicated order, or a general power of search and seizure.

To express 'seriousness' and to reduce 'penalty havens' – From an international cooperation perspective, penalties specified for criminal offences do not strictly require harmonization on the same grounds as for substantive criminal law and the coercive powers of criminal procedural law. Dual criminality does not concern the respective sanctions. Nonetheless, there is a special nexus between cooperation and the level of punishment. The penalties assigned to a crime are indicative of the level of *seriousness* of the offence. At the international level, the Organized Crime Convention, for example, defines 'serious crime' as conduct constituting an offence '*punishable by a maximum deprivation of liberty of at least four years or a more serious penalty*.'[46] Given the significant investment that international cooperation requires of States, many extradition instruments specify a threshold of seriousness for the crime involved – usually expressed with reference to the possible penalty that the offence may attract.[47] Seriousness thresholds also represent an important mechanism for the protection of the principle of proportionality and the rights of the accused.[48] Similar requirement may also apply in some agreements on mutual legal assistance.[49]

Typical penalty thresholds found in international cooperation instruments range from six months,[50] to one year,[51] or four years.[52] During information gathering for the Study, countries were asked about penalties that applied to a range of cybercrime acts, including acts against the

---

44 See De Bondt, W., 2012. *Need for and feasibility of an EU offence policy*. Antwerp: Maklu, pp. 46-47.

45 It is not usually explicitly stated in instruments governing mutual assistance that measures which do not exist in the requested state should nonetheless be executed. For coercive measures, however, the draft European Investigation Order states that alternative measures can and should be used when the requested measure does not exist under the law of the requested state. See Council of Europe. 2011. *Initiative for a Directive regarding the European Investigation Order in criminal matters* – Text agreed as general approach, 18918/11, 21 December 2011, pp.19-20.

46 Organized Crime Convention, Art. 2. The four year threshold is used to define a general category of 'serious crime' to which the Convention applies (which also must be transnational in nature and involve an organized criminal group). The threshold does not apply to the specific offences also established in the Convention.

47 Schwaighofer, K., Ebensperger S., 2001. *Internationale Rechtshilfe in strafrechtlichen Angelegenheiten.* Vienna: WUV Universitätsverlag, p. 8.

48 Lagodny, O. 2012. *In:* Schomburg, W., Lagodny, O., Gless, S., Hackner, T. (eds.) *Internationale Rechtshilfe in Strafsachen.* Munich: C.H.Beck, p.90 § 3 IRG, at 23; Murschetz, V. 2007. *Auslieferung und Europäischer Haftbefehl.* Vienna/New York: Springer, p.124.

49 Article 5(1)(b) of the Council of Europe Convention on Mutual Assistance in Criminal Matters, for example, provides that any contracting party may require an extraditable offence in order to execute letters rogatory for search or seizure of property.

50 Article 2(1) of the Convention on Extradition of the European Union provides that an offence is extraditable if it is punishable by deprivation of liberty of at least one year under the law of the request*ing* state and at least six months in the request*ed* state. Note, however, that the Convention has been largely replaced by the European Arrest Warrant (Hackner, T., 2012. *In:*, Schomburg, W., Lagodny, O., Gless, S., Hackner, T. (eds.) *Internationale Rechtshilfe in Strafsachen.* Munich: C.H.Beck. p.1174, III A, at 3, and pp.1178-1179, III A 1, at 9).

51 The extradition provisions of the Council of Europe Cybercrime Convention, for example, apply to criminal offences established in accordance with Articles 2 to 11 of the Convention, provided that they are punishable under the laws of both parties by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.

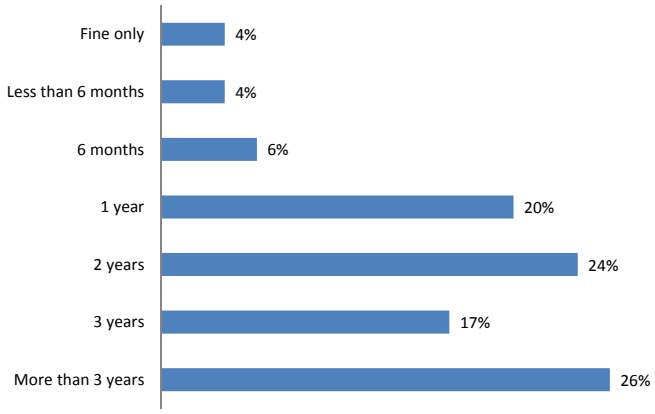
52 Organized Crime Convention, Arts. 2 and 16.

confidentiality, integrity and availability of computer data and systems, computer-related acts for personal or financial gain, and specific computer-related acts.[53]

Figures 3.4 and 3.5 show the distribution of penalties for the acts of 'mere illegal access' to a computer system or computer data, and for the same crime – but where 'bypassing security' or 'dishonest intent' is required by the national legal provision.[54]

For both crimes, it is apparent that a number of countries provide for maximum penalties of less than one year. In light of the fact that one year is typically the most common threshold for extradition purposes (and the one used by instruments such as the Council of Europe Cybercrime Convention, and the League of Arab States Convention), international cooperation in respect of these offences (alone) in some countries may prove challenging.[55] The typical sentences are certainly well below the four year 'serious crime' threshold used in the Organized Crime Convention.

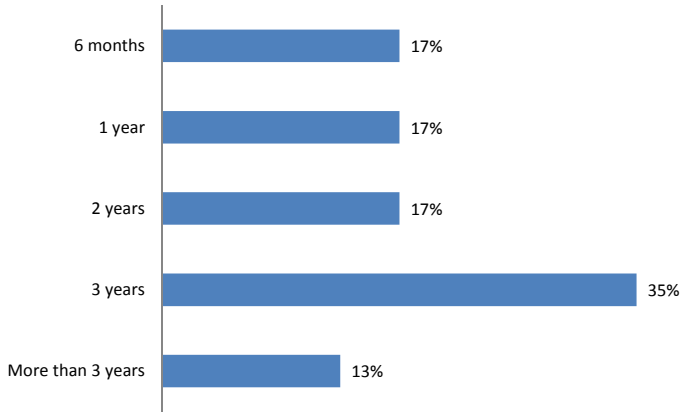
Figure 3.4: Mere illegal access to computer system or data maximum term of imprisonment



Source: UNODC legislation review. (n=54)

Such results must be interpreted with caution, however, regarding the picture of penalties applied *in practice*. Penalty levels in practice cannot easily be assessed solely with reference to specific criminal law provisions. Rather, they may be affected by general rules on sentencing, on aggravating and mitigating circumstances, or by specific qualifications and sentencing guidelines.

Figure 3.5: Illegal access (bypassing security or dishonest intent) maximum term of imprisonment



Source: UNODC legislation review (n=23)

Nonetheless, the picture serves to highlight the general challenges encountered when it comes to defining the *scope* of international cooperation and common agreement on cybercrime offence *seriousness*. On the one hand, the act of 'mere illegal access' could cover comparatively minor conduct. On the other hand, illegal access represents the starting point for many serious cybercrime acts,

53 Study cybercrime questionnaire. Q25-39. Information on penalties was also gathered by the Secretariat from additional sources included in the primary source legislation review.

54 Analysis limited to countries in which the maximum penalty is indicated in the specific legal article (thus not including countries for which the punishment can only be determined by analysing general provisions of the criminal code).

55 Although note that responding countries also reported that cybercrime acts *are* widely considered to meet seriousness standards and to constitute extraditable offences. All responding countries in Europe and the Americas, and 90 per cent of countries in Africa, Asia and Oceania reported that cybercrime acts are, in general, extraditable offences (Study cybercrime questionnaire. Q194). The discrepancy likely arises from the fact that it is rare for perpetrators to be charged with, and extradition sought, for 'illegal access' in isolation from other charges.

and can include intentional unauthorized entry to computer systems – such as those used for critical national infrastructure. Reference to the 'maximum' possible penal sentence for the purposes of determining cooperation thresholds does not necessarily well characterize the act itself. Alternative approaches, such as defining a list of specific crimes to which international cooperation provisions apply (without a need for penal thresholds), suffer from the limitations of restricted scope. Overall, broad harmonization of penalties between countries for specific core cybercrime offences – including common seriousness-based penalty levels – likely could assist in facilitating international cooperation and the elimination of 'penalty havens' for perpetrators.

Summary

The current picture of cybercrime legislation is a dynamic one – indicating ongoing legal reform and increasing recognition that cybercrime requires a legal response across multiple areas: criminal, civil and administrative. Almost 60 per cent of responding countries indicated new or planned cybercrime legislation in their response to the Study questionnaire.[56] While 'traditional' general law can be applied to cybercrime matters to some extent, the intangible nature of concepts such as 'computer data' also requires the introduction of specific offences, definitions, and concepts – if legal interests such as the integrity of computer systems are to be protected.

While consensus exists about broad areas of legal intervention for the prevention and combating of cybercrime, levels of harmonization of legislation as between countries viewed as important for cooperation, within regions, and with multilateral instruments, are perceived to be highly variable. This includes in the area of cybercrime offence penalties, where an examination of one foundational crime – illegal access – shows divergence to the extent that smooth international cooperation concerning this crime may be affected. Harmonization itself is required for reasons, amongst others, of the elimination of criminal safe havens, and for global evidence collection. Routes to harmonization include the use of binding and non-binding international and regional instruments. As alluded to in the Study thus far, many such instruments exist. The next section of this Chapter examines these in detail.

3.3 Overview of international and regional instruments

Key results:

- The last decade has seen significant developments in the promulgation of international and regional instruments aimed at countering cybercrime. These include binding and non-binding instruments
- Five clusters of international or regional instruments can be identified, consisting of instruments developed in the context of, or inspired by: (i) the Council of Europe or the European Union, (ii) the Commonwealth of Independent States or the Shanghai Cooperation Organization, (iii) intergovernmental African organizations, (iv) the League of Arab States, and (v) the United Nations
- A significant amount of cross-fertilization exists between all instruments, including, in particular, concepts and approaches developed in the Council of Europe Cybercrime Convention
- Analysis of provisions of 19 multilateral instruments relevant to cybercrime shows common core provisions, but also significant divergence in substantive areas addressed

[56] Study cybercrime questionnaire. Q14.

The last decade has seen significant developments in the promulgation of international and regional instruments aimed at countering cybercrime. The genesis, legal status, geographic scope, substantive focus, and mechanisms of such instruments vary significantly.

Five possible 'clusters' of instruments may be identified – (i) instruments developed in the context of, or inspired by, the Council of Europe or the European Union; (ii) instruments developed in the context of the Commonwealth of Independent States or the Shanghai Cooperation Organization; (iii) instruments developed in the African context; (iv) instruments developed by the League of Arab States, and (v) instruments developed under the auspices of, or associated with, United Nations entities.

These clusters are not absolute and a significant amount of cross-fertilisation exists between the instruments. The basic concepts developed in the Council of Europe Cybercrime Convention, for example, are also found in many other instruments.[57] United Nations entities, such as UNECA and ITU, have also had some involvement in the development of instruments in the African context, including the Draft African Union Convention and the SADC Model Law.

Within a cluster, instruments may have a particularly direct relationship. The Commonwealth Model Law, for example, is based closely on the Council of Europe Cybercrime

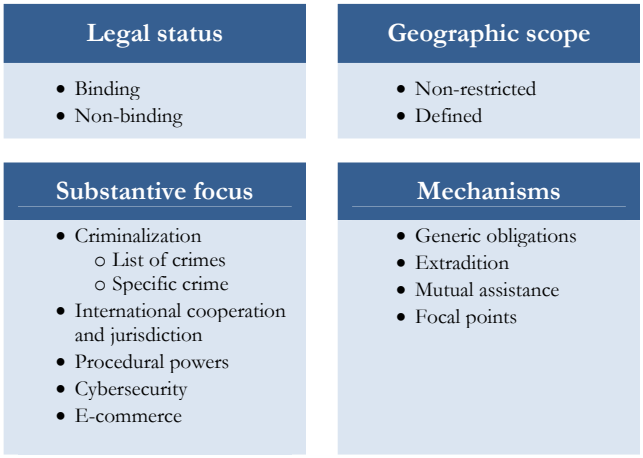
Binding	Non-binding
▪ Council of Europe Convention on Cybercrime (2001) and Additional Protocol (2003) ▪ Council of Europe Convention on Protection of Children against Sexual Exploitation and Sexual Abuse (2007) ▪ EU legislation including on e-Commerce (2000/31/EC), on Combating Fraud and Counterfeiting of Non-Cash Means of Payment (2001/413/JHA), on Personal Data (2002/58/EC as amended), on Attacks against Information Systems (2005/222/JHA and Proposal COM(2010) 517 final), and on Child Pornography (2011/92/EU)	▪ Commonwealth Model Laws on Computer and Computer-related Crime (2002) and Electronic Evidence (2002)
▪ Commonwealth of Independent States (CIS) Agreement on Cooperation in Combating Offences related to Computer Information (2001) ▪ Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security (2009)	
▪ (Draft) Economic Community of West African States (ECOWAS) Directive on Fighting Cybercrime (2009) ▪ (Draft) African Union Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa (2012)	▪ East African Community Draft Legal Framework for Cyberlaws (2008) ▪ Common Market for Eastern and Southern Africa (COMESA) Cybersecurity Draft Model Bill (2011) ▪ Southern African Development Community (SADC) Model Law on Computer Crime and Cybercrime (2012)
▪ League of Arab States Convention on Combating Information Technology Offences (2010)	▪ League of Arab States Model Law on Combating Information Technology Offences (2004)
▪ Optional Protocol to the United Nations Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (2000)	▪ International Telecommunication Union (ITU)/Caribbean Community (CARICOM)/Caribbean Telecommunications Union (CTU) Model Legislative Texts on Cybercrime, e-Crime and Electronic Evidence (2010) ▪ International Telecommunication Union (ITU)/Secretariat of the Pacific Community Model Law on Cybercrime (2011)

[57] The analysis contained in Annex Three to this Study ('Provisions of international and regional instruments') demonstrates that many key concepts found in the Council of Europe Cybercrime Convention – such as illegal access to a computer system, illegal interception of computer data, illegal interference with computer data or a computer system, expedited preservation of computer data, and real-time collection of computer data – are also found in other, later, instruments.

Convention. The Draft African Union Convention incorporates language from the ECOWAS Draft Directive, and the Commonwealth of Independent States Agreement and Shanghai Cooperation Organization Agreement show some common concepts related to computer information security.

Similarities and differences between the instruments and clusters can be illustrated with reference to the schema below, focusing on 'legal status', 'geographic scope', 'substantive focus', and 'mechanisms.'

Legal status



A first important distinction concerns whether an instrument is legally binding. A number of the instruments – notably the Council of Europe Conventions, the European Union instruments, the Commonwealth of Independent States Agreement, the Shanghai Cooperation Organization Agreement, and the League of Arab States Convention – are express agreements between states intended to create legal obligations.[58] If approved by the Assembly of the African Union, the Draft African Union Convention would also be open for signature, ratification or accession, with entry into force in the form of a binding instrument.[59]

Other instruments – such as the Commonwealth Model Law, the COMESA Draft Model Bill, the League of Arab States Model Law, and the ITU/CARICOM/CTU Model Legislative Texts – are not intended to create legal obligations for states. Rather, they are designed to serve as inspiration or 'models' for development of national legislative provisions. Non-binding instruments may nonetheless have a significant influence at the global or regional level when many states choose to align their national laws with model approaches.[60] In addition, countries that have not ratified or acceded to a binding instrument may nonetheless make use of a binding instrument as inspiration for national legislative provisions – with the result that the reach of an instrument can be broader than the number of countries that have signed, ratified or acceded.[61]

Geographic scope

For binding instruments, the geographic scope is typically determined by the nature and

---

58 'International conventions', whether general or particular, establishing rules expressly recognized, are included as a source of international law to be applied by the International Court of Justice under Article 38 of the Statute of the International Court of Justice. Article 2 of the Vienna Convention on the Law of Treaties defines a 'treaty' as an 'international agreement concluded between States in written form and governed by international law, whether embodied in a single instrument or in two or more related instruments and whatever its particular designation.'

59 Draft African Union Convention. Part IV, Section 2. In September 2012, the 4th Ordinary Session of the African Union Conference of Ministers in Charge of Communication and Information Technologies (CITMC-4) requested the Draft African Union Convention to be submitted by the African Union Commission for adoption according to African Union rules of procedure. See African Union. 2012. *Khartoum Declaration*. AU/CITMC-4/MIN/Decl.(IV)Rev 2, 6 September 2012.

60 A number of states in the Commonwealth, for example, have used provisions from the Commonwealth Model Law either alone, or in conjunction with the Council of Europe Cybercrime Convention. See Council of Europe. 2012. *Commonwealth States: Use of the Budapest Convention and Commonwealth Model Law. Council of Europe's contribution to the Commonwealth Working Group on Cybercrime.*

61 The Council of Europe, for example, reports that, in addition to the countries that have ratified, signed or been invited to accede to the Council of Europe Cybercrime Convention, it has engaged with at least 55 countries in technical cooperation on the basis of the Convention. See Seger, A., 2012. The Budapest Convention on Cybercrime 10 years on: Lessons learnt or the web is a web.

context of the organization under whose auspices the instrument is developed. Thus, for example, the League of Arab States Convention has as its purpose 'to enhance and strengthen cooperation between the *Arab States.*'[62] Similarly, the Commonwealth of Independent States Agreement defines 'the Parties' as the '*States members of the Commonwealth of Independent States,*'[63] and the Draft African Union Convention is envisaged to be open to '*Member States of the African Union.*'[64]

Instrument membership does not necessarily coincide with organizational membership. Not all members of the organization may be signatory to the original agreement,[65] and – where the agreement is subject to ratification, acceptance or approval[66] – not all signatories may have deposited such instruments.[67] Some instruments are opened for signature outside of the membership of the organization under whose auspices the instrument was developed. The Council of Europe Cybercrime Convention, for example, was open for signature by member states of the Council of Europe and by '*non-member States which have participated in its elaboration.*'[68]

Founding states become the incumbent states that control entry of new states applying for accession, often according to rules set forth in the initial treaty agreement.[69] Treaties may be 'open' in that any state may accede by simply expressing their intent to be bound to the existing treaty terms; 'semi-open' where expansion can be approved by a majority of signatory and/or contracting states; or 'closed' where expansion requires unanimous approval of signatory and/or contracting states.[70]

With respect to the Council of Europe Cybercrime Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the contracting states to the Convention, may '*invite any State which is not a member of the Council and which has not participated in its elaboration to accede to* [the] *Convention.*'[71] Similarly, the Commonwealth of Independent States Agreement is '*open for accession by any other State willing to be bound by its provisions, subject to the agreement of all Parties.*'[72] The Shanghai Cooperation Organization Agreement also provides that it is '*open to accession by any State that shares the goals and principles of* [the] *Agreement.*'[73] Instruments developed under the auspices of the United Nations typically have the broadest

---

62 League of Arab States Convention, Art. 1.

63 Commonwealth of Independent States Agreement. Preamble.

64 Draft African Union Convention. Part IV, Section 2, Art. IV-2.

65 League of Arab States members Comoros, Djibouti, Lebanon, and Somalia have not signed the League of Arab States Convention. Council of Europe member states Andorra, Monaco, the Russian Federation, and San Marino have not signed the Council of Europe Cybercrime Convention.

66 Article 14 of the Vienna Convention on the Law of Treaties provides that '*The consent of a State to be bound by a treaty is expressed by ratification when: (a) the treaty provides for such consent to be expressed by means of ratification; (b) it is otherwise established that the negotiating States were agreed that ratification should be required; (c) the representative of the State has signed the treaty subject to ratification; or (d) the intention of the State to sign the treaty subject to ratification appears from the full powers of its representative or was expressed during the negotiation.*' The Council of Europe Cybercrime Convention and the League of Arab States Convention expressly provide that the agreement is subject to ratification, acceptance or approval. The Commonwealth of Independent States Agreement and the Shanghai Cooperation Organization Agreement envisage the deposit of notification that parties have completed internal procedures required for entry of the agreement into force. The Draft African Union Convention envisages signature, ratification or accession. For a review of international law of treaties in general see Shaw, M.N., 2007. *International Law*. 6th ed. Cambridge: Cambridge University Press.

67 Council of Europe Cybercrime Convention signatories Czech Republic, Greece, Ireland, Liechtenstein, Luxembourg, Poland, Sweden and Turkey have not yet deposited instruments of ratification, acceptance or approval.

68 Council of Europe Cybercrime Convention, Art. 36(1). Non-member states Canada, Japan, South Africa and the United States of America signed the Council of Europe Cybercrime Convention.

69 Article 15 of the Vienna Convention on the Law of Treaties provides that '*The consent of a State to be bound by a treaty is expressed by accession when: (a) the treaty provides that such consent may be expressed by that State by means of accession; (b) it is otherwise established that the negotiating States were agreed that such consent may be expressed by that State by means of accession; or (c) all the parties have subsequently agreed that such consent may be expressed by that State by means of accession.*'

70 Malone, L.A., 2008. *International Law*. New York: Aspen.

71 Council of Europe Cybercrime Convention, Art. 37(1). Proposals for amendment of the procedure followed under Art. 37(1) have been made by the Council of Europe Cybercrime Convention Committee (T-CY) and the European Committee on Crime Problems (CDPC). Both proposals are currently under review by the Council of Europe Rapporteur Group on Legal Co-operation (GR-J). See Council of Europe Cybercrime Convention Committee 2012. *Criteria and Procedures for Accession to the Budapest Convention on Cybercrime – Update*. T-CY (2012)12 E. 28 May 2012.

72 Commonwealth of Independent States Agreement, Art. 17.

73 Shanghai Cooperation Organization Agreement, Art. 12.

geographical scope. The Convention on the Rights of the Child and its Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography, for instance, is open for '*accession by any State.*'[74]

Founding states have the advantage of influencing the content of the treaty, yet may face certain costs in the process of treaty negotiation and drafting. Accession to treaties at a later stage avoids such costs but offers limited opportunities for renegotiation of treaty obligations and content. In so far as treaties are often concluded by states with similar preferences, treaties may not be acceptable to states that were not involved in negotiations, even if the treaty is left open for accession.[75]

Multilateral treaties typically recognize this through a system of reservations that may be made at the time of signature, ratification or accession.[76] The Council of Europe Cybercrime Convention permits specified reservations concerning particular articles, although no other reservations may be made.[77] The League of Arab States Convention permits specified reservations, and prohibits only reservations '*involving a violation of the texts of the Convention or a departure from its objectives.*'[78] The Commonwealth of Independent States Agreement is silent on the issue of reservations,[79] and at least one country has entered a reservation.[80] If adopted in its current form, the African Union Convention would allow reservations concerning '*one or several specific provisions*' that are '*not incompatible with the objectives and purposes of* [the] *Convention.*'[81]

Globally, 82 countries have signed and/or ratified one of the binding cybercrime instruments.[82] Some countries are members of more than one such instrument. Despite the possibility of participation beyond the original organisational or drafting context, Figure 3.6[83] shows that – to date – no single instrument (apart from the United Nations OP-CRC-SC[84]) has received signatures or ratifications/accessions with global geographic reach. The Council of Europe Cybercrime Convention has the largest number of signatures or ratifications/accessions (48 countries), including five Non-member States of the Council of Europe.[85] Other instruments have smaller geographic scope – the League of Arab States Convention (18 countries or territories), the Commonwealth of Independent States Agreement (10 countries), and the Shanghai Cooperation Organization Agreement (6 countries). If signed or ratified by all member states of the African

---

74 United Nations Convention on the Rights of the Child, Art. 48; and United Nations OP-CRC-SC, Art. 13. 'State' has a broad meaning in this content and is not limited to Member States of the United Nations. The Holy See, for example, as a Non-member State of the United Nations, has both signed and ratified the Convention on the Rights of the Child, and the OP-CRC-SC. See http://treaties.un.org/Pages/Treaties.aspx?id=4&subid=A&lang=en

75 Parisi, F., Fon, V., 2009. The Formation of International Treaties. *In: The Economics of Lawmaking*. Oxford: Oxford Scholarship Online.

76 Section 2 of the Vienna Convention on the Law of Treaties addresses the formulation of reservations, acceptance of and objection to reservations, the legal effects of reservations and objections to reservations, the withdrawal of reservations and of objections to reservations, and procedure regarding reservations. In general, reservations that are incompatible with the 'object and purpose' of the treaty are not permissible.

77 Council of Europe Cybercrime Convention, Art. 42.

78 League of Arab States Convention, Chapter V, Art. 6.

79 Under Article 24 of the Vienna Convention on the Law of Treaties, the default position is that a state may formulate reservations unless specifically prohibited by the treaty, or when the treaty provides for only specified reservations, or when the reservation is incompatible with the object and purpose of the treaty.

80 Reservation of Ukraine under item 5 of the agenda of the meeting of the Council of Heads of States Members of the Commonwealth of Independent States, entitled '*Agreement on cooperation in combating offences related to computer information*' 1 June 2001.

81 Draft African Union Convention, Part IV, Section 2, Art. IV-3.

82 Signature or ratification of: Council of Europe Cybercrime Convention, League of Arab States Convention, Commonwealth of Independent States Agreement, and Shanghai Cooperation Organization Agreement.

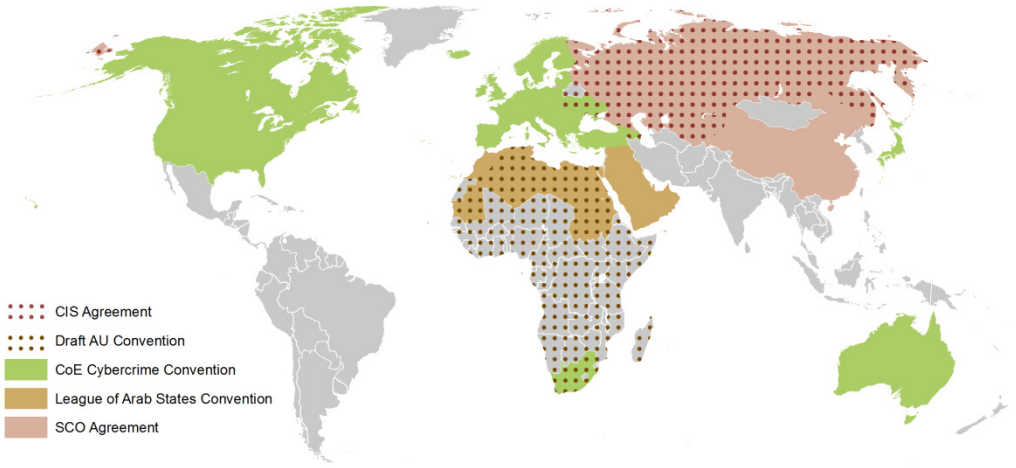
83 The map shows all countries that have either signed, ratified, or acceded to the Commonwealth of Independent States Agreement (CIS), the Council of Europe Cybercrime Convention (CoE), the League of Arab States Convention (LAS), and the Shanghai Cooperation Organization Agreement (SCO). For reference, the map also depicts membership of the African Union, representing the possible total membership of the Draft African Union Convention, if agreed and opened for signature, ratification or accession.

84 176 countries or territories have signed, ratified or acceded to the United Nations OP-CRC-SC.

85 In addition, a further eight countries (Argentina, Chile, Costa Rica, Dominican Republic, Mexico, Panama, Philippines, and Senegal) have been invited to accede to the Council of Europe Convention in accordance with the provisions of Article 37. Accession of these countries to the Convention would significantly expand its geographic scope.

Union, the Draft African Union Convention could have up to 54 countries or territories.

Figure 3.6: International and regional instruments

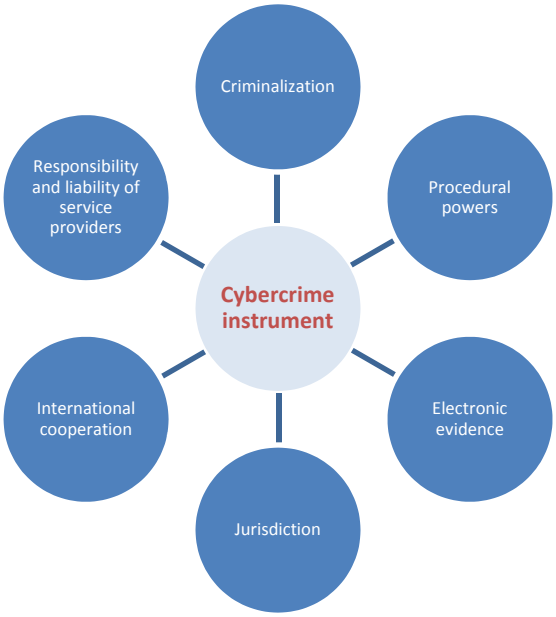


Overall, the global picture is one of a certain degree of fragmentation in membership of international and regional instruments related to cybercrime. Regional patterns are particularly clear. Countries in some parts of the world benefit from membership of binding cybercrime instruments – including more than one instrument for some countries – while other regions do not participate in any binding framework.

Substantive focus

In addition to differences in geographic scope, international and regional instruments also show – in the same way as national legislation – differences in substantive focus. Many of these differences derive from the underlying aim of the instrument. Some instruments, such as the Council of Europe Cybercrime Convention, the Commonwealth Model Law, the League of Arab States Convention, and the Commonwealth of Independent States Agreement, aim specifically to provide a criminal justice framework for combating forms of cybercrime. Others, such as the Shanghai Cooperation Organization Agreement and the Draft African Union Convention, take a broader approach, of which cybercrime is just one component. The Shanghai Cooperation Organization Agreement, for example, addresses cooperation in cybercrime matters within the context of international information security – including information warfare, terrorism and threats to global and national information

Figure 3.7: Substantive focus of cybercrime instruments



infrastructures.[86] The Draft African Union Convention takes a cybersecurity-based approach that includes organization of electronic transactions, protection of personal data, promotion of cybersecurity, e-governance and combating cybercrime.[87]

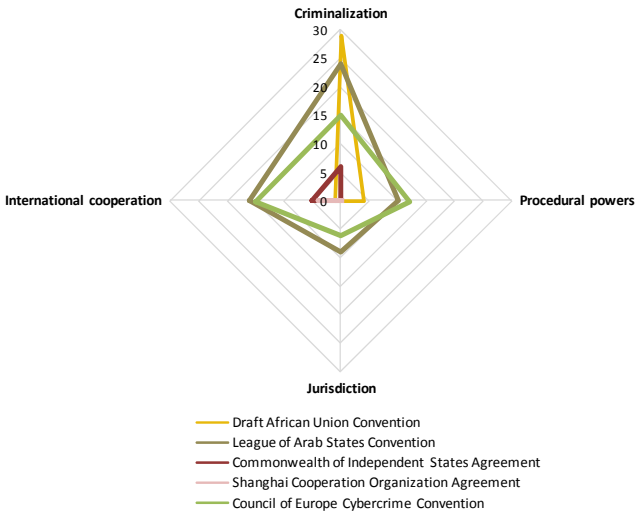
Such differences significantly affect the way in which cybercrime is 'framed' within the international or regional legal response. Due to its broader focus on international information security, for example, the Shanghai Cooperation Organization Agreement does not set out specific cyber acts that should be criminalized. Similarly – perhaps due to its focus on cybersecurity as a whole, rather than criminal justice in particular – the Draft African Union Convention presently does not seek to establish mechanisms of international cooperation in cybercrime criminal matters.

From the crime prevention and criminal justice perspective, six key areas may benefit from either binding or non-binding guidance at international or regional level: (i) criminalization; (ii) law enforcement procedural powers; (iii) procedures regarding electronic evidence; (iv) state jurisdiction in cybercrime criminal matters; (v) international cooperation in cybercrime criminal matters; and (vi) the responsibility of service providers.

The substance of international and regional instruments – and, indeed, national laws – in each of these areas can be analysed on three levels: (1) the *existence* of relevant provisions in each area; (2) the *coverage* of the provisions *within* each area; and (3) the *content* of provisions. This section is concerned with levels one and two. Level three is examined in Chapter Four (Criminalization) and Chapter Five (Law enforcement and investigations).

With respect to the *existence* of relevant provisions, the binding and non-binding international and regional instruments identified address the six areas to different extents. Provisions on criminalization, procedural powers, jurisdiction and international cooperation are commonly found in a number of binding instruments. In contrast, provisions on electronic evidence and service provider responsibility are more commonly addressed in non-binding instruments – such as the Commonwealth Model Law, the COMESA Draft Model Bill, and the ITU/CARICOM/CTU Model Legislative Texts.[88] Only the (envisaged to be binding) ECOWAS Draft Directive and the Draft African Union Convention contain provisions relevant to electronic evidence.[89] Similarly, only European Union legislation addresses the issue of service

Figure 3.8: Structure of international and regional instruments



[86] Article 2 of the Shanghai Cooperation Organization Agreement includes cybercrime as a 'major threat' to international information security. 'Cybercrime' is defined in Annex 1 to the Agreement as '*the use of information resources and (or) the impact on them in the information space for illegal purposes*.'

[87] In the Draft African Union Convention, cybercrime is addressed in Part Three: '*Promoting cybersecurity and combating cybercrime*.' Parts One and Two address '*Electronic transactions*' and '*Personal data protection*', respectively.

[88] See tables 'Electronic evidence' and 'Service provider liability and responsibility' at Annex Three to this Study.

[89] See ECOWAS Draft Directive, Art. 34, and Draft African Union Convention, Art. I(24).

provider liability and responsibility at regional or international level.[90]

Within the areas of criminalization, law enforcement procedural powers, and international cooperation, the instruments also show a range of approaches. Figure 3.8 demonstrates the relative distribution of the number of articles within five binding international or regional instruments that address each area. Instruments such as the Council of Europe Cybercrime Convention and the League of Arab States Convention cover all four areas. The Draft African Union Convention is focussed heavily on criminalization with the inclusion of some procedural powers. The Commonwealth of Independent States Agreement includes a small number of articles on international cooperation and criminalization. Out of the four areas, the Shanghai Cooperation Organization Agreement contains only articles on international cooperation.

The *coverage* of relevant provisions within instruments also varies significantly. Annex Three to this Study contains a complete analysis of the coverage of provisions in each of the six key areas, by instrument. The analysis shows diversity in the range of conduct criminalized by the instruments, in the breadth of law enforcement procedural powers, and in the approaches to jurisdiction and international cooperation. Annex Three also demonstrates that – while important differences do exist – many instruments nonetheless share certain 'core' provisions. These include, in particular: the criminalization of acts against the confidentiality, integrity and availability of computer data or systems; procedural powers including search, seizure, orders for computer data, real-time collection of computer data, and preservation of data; and general obligations to cooperate in the investigation of cybercrime criminal matters. The Table below summarizes some of the key results from the analysis at Annex Three.

Criminalization	• Most instruments contain an extensive list of offences. Others focus only on a limited thematic offence area, such as instruments focusing on child pornography and child protection • Acts against the confidentiality, integrity and availability of computer data or systems are most commonly criminalized, followed by computer-related fraud or forgery, and computer-related production, distribution or possession of child pornography • In addition to the acts identified in Chapter One of this Study in the section on 'Describing cybercrime', some instruments also criminalize a wide range of acts, including computer-related offences against public order, morality or security • Some instruments provide that conventional crimes committed by means of a computer system should be an aggravating circumstance
Procedural powers	• Search, seizure, orders for stored computer data and subscriber information, real-time collection of computer data, and expedited preservation of computer data are the most common procedural powers • Trans-border access to computer data is envisaged by three instruments
Electronic evidence	• The few (mainly, non-binding) instruments that address electronic evidence cover areas including the general admissibility of electronic evidence, the burden of proving authenticity, the best evidence rule, the presumption of integrity, and preservation standards
Jurisdiction	• Nearly all instruments include the territorial principle and nationality principle (where dual criminality exists) as bases for jurisdiction • Other bases for jurisdiction, not found in all instruments, include acts directed against a computer system or data located within the territory and a state interests principle • Two instruments provide guidance on establishment of the place of a cybercrime offence

[90] See, for example, EU Directive on e-Commerce, Arts. 12 to 15.

International cooperation	• Instruments tend to either address international cooperation extensively – providing mechanisms for mutual legal assistance and extradition – or to focus in a more limited way on general principles of cooperation • A number of instruments envisage the establishment of points of contact or 24/7 networks
Service providers	• The limited number of instruments that address the responsibility of service providers cover areas including monitoring obligations, voluntary supply of information, take-down notifications, and liability of access, caching, hosting and hyperlink providers

Mechanisms

Mechanisms of international cooperation are particularly relevant to *binding* international or regional instruments – as these are able to provide a clear international legal obligation or power for cooperation amongst states parties. In addition to general obligations to cooperate,[91] a number of instruments – notably the Commonwealth of Independent States Agreement, the Council of Europe Convention, and the League of Arab States Convention – establish concrete mechanisms for cooperation. For each of these three agreements, the instrument itself may be relied upon as the basis for requests for assistance from one state party to another.[92] As such, the instrument may also, without prejudice to conditions provided for by national law or other applicable mutual assistance treaties, set out the reasons for which a state party may refuse assistance.[93] The Commonwealth of Independent States Agreement uses the approach of defining the types of assistance that may be requested in rather broad terms.[94] The Council of Europe Cybercrime Convention and the League of Arab States Convention, in addition to general obligations to afford mutual assistance to the widest extent possible for the purpose of investigations or proceedings, also include specific forms of assistance – such as expedited preservation of stored computer data, expedited disclosure of preserved traffic data, accessing of stored computer data, real-time collection of traffic data, and interception of content data.[95]

Finally, a number of instruments establish registers of competent authorities for the purposes of extradition and mutual legal assistance requests,[96] procedures for expedited assistance,[97]

---

91 See for example, Article 23 of the Council of Europe Cybercrime Convention which provides that '*The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems or data, or for the collection of evidence in electronic form of a criminal offence.*'

92 See, for example, Article 27 of the Council of Europe Cybercrime Convention, which provides that '*Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of hits article shall apply*'; Article 34 of the League of Arab States Convention, which provides that '*The provisions of paragraphs 2 through 9 of this Article shall apply in case no cooperation and mutual assistance treaty or convention exists on the basis of the applicable legislation between the States Parties requesting assistance and those from which assistance is requested*'; and Article 6 of the Commonwealth of Independent States Agreement, which provides that '*Cooperation within the framework of this Agreement shall be based on requests for assistance made by the competent authorities of the Parties.*'

93 See, for example, Council of Europe Cybercrime Convention, Art. 27(4), and the League of Arab States Convention, Art. 35, both of which provide that assistance may be refused if the request is considered to relate to a political offence, or if the requested state considers that the request is likely to prejudice its sovereignty, security, public order or other essential or basic interests.

94 Article 5 of the Commonwealth of Independent States Agreement includes, for example, exchange of information on offences relating to computer information that are in the course of preparation or have been committed; the execution of requests for investigations and proceedings in accordance with international instruments on legal assistance; and the planning and implementation of coordinated activities and operations to prevent, detect, suppress, uncover and investigate offences relating to computer information.

95 See Council of Europe Cybercrime Convention, Arts. 29, 30, 31, 33 and 34; and League of Arab States Convention, Arts. 37-39, 41 and 42.

96 See Council of Europe Cybercrime Convention, Arts. 24(7) and 27(2); Commonwealth of Independent States Agreement, Art. 4; and League of Arab States Convention, Arts. 31(7) and 34(2).

97 See Council of Europe Cybercrime Convention, Art. 31(3); Commonwealth of Independent States Agreement, Art. 6(2); and League of Arab States Convention, Art. 34(8).

and focal points for the provision of 24 hours a day communication channels.[98]

3.4 Implementing multilateral instruments at the national level

Key results:

- In addition to formal membership and implementation, multilateral cybercrime instruments have influenced national laws indirectly, through use as a model by non-States parties, or via the influence of legislation of States parties on other countries
- Membership of a multilateral cybercrime instrument corresponds with the perception of increased sufficiency of national criminal and procedural law, indicating that current multilateral provisions in these areas are generally considered effective
- Fragmentation at the international level, and diversity of national laws, in terms of cybercrime acts criminalized, jurisdictional bases, and mechanisms of cooperation, may correlate with the existence of multiple cybercrime instruments with different thematic and geographic scope

The manner in which international or regional instruments are implemented in national law, as well as the effectiveness of the application and enforcement of new rules, can be decisive factors in the success, or otherwise, of harmonization.[99] States may interpret or implement the provisions of international instruments in different ways, leading to further divergence across countries. This, in itself, is not a problem: countries will not always implement international frameworks in exactly the same way, due to different legal traditions and limitations that exist at the national level.[100] At the same time, however, the goal of implementation is to provide a certain degree of compliance of national legislation with international frameworks.

Vertical (direct) implementation

'Direct' implementation of a multilateral treaty follows signature and ratification of, or accession to, a treaty. For most international rules to become operative, they must be applied by State officials or individuals within domestic legal systems. States may achieve this either through 'standing incorporation' of international rules into domestic law (often associated with so-called 'monist' systems) or by 'legislative incorporation'

Implementation of the EU Decision on Attacks against Information Systems

A report on the implementation of the EU Framework Decision on Attacks against Information Systems (2005) reveals significant divergence in the use of the option not to criminalize 'minor cases.' Member states, for example:

- Criminalized access only with the intent to perpetrate data espionage;
- Criminalized illegal access only in cases where the data was subsequently misused or damaged;
- Established a condition of endangering the data accessed as a requirement for criminal responsibility.

The report on implementation pointed out that, in general, '*such a divergence of interpretation and application of the option not to criminalize certain acts poses a serious risk to the objective to approximate Member State rules on criminal law in the area of attacks against information systems.*'

Source: European Commission. 2008. COM (2008) 448 final.

98 See Council of Europe Cybercrime Convention, Art. 35 and League of Arab States Convention, Art. 43.

99 Miquelon-Weismann, M. F., 2005. The Convention on Cybercrime: A Harmonized Implementation of International Penal Law: What Prospects for Procedural Due Process? *John Marshall Journal of Computer & Information Law*, 23(2):329-61.

100 See Klip, A., Nelken, D., 2002. Changing Legal Cultures. *In*: Likosky, M. (ed.) *Transnational Legal Processes*. London: Butterworths; Graziadei, M., 2009. Legal Transplants and the Frontiers of Legal Knowledge. *Theoretical Inquiries in Law*, 10(2): 723-743.

(in 'dualist' systems), whereby international rules become applicable within the national legal system only if and once the relevant national legislation is passed.[101]

The incorporation of cybercrime instrument provisions into national law will often involve amendment of legislation such as the criminal code and criminal procedure code in order either to introduce new specific offences, or to amend existing ones.

The result in national law may be significantly different from State party to State party. A specific effect that the implementation of an international instrument has on the national legal system of one state, for example, may never occur in another.[102] An assessment of the implementation of the EU Decision on Attacks against Information Systems[103] illustrates well the challenges faced in harmonization of cybercrime legislation – even in the context of a binding framework and countries accustomed to implementation of supra-national law.[104] As illustrated in the box, assessment of implementation showed significant divergences in national legal provisions designed to implement the Decision. The assessment also highlights a further point – that review of implementation of any instrument is a technical and challenging process, requiring time, resources and full information on both legislative provisions, and their application in practice.[105] It is beyond the scope and mandate of this Study to carry out any form of assessment of implementation of the different international and regional cybercrime instruments referred to in this Chapter.

Implementation of the ECOWAS Draft Directive

In 2008, a country in Western Africa adopted a law concerning regulations provided at the regional level by ECOWAS on cybercrime. The specific amendments included:

- Creation of IT-specific offences in the fields of criminal protection of IT systems and electronic data, illegal content, computer fraud, technical assistance services, and digital advertising;
- Updating of legislation on existing offences to make it relevant to the new IT/telecommunications environment (in the fields of criminal protection against theft, physical damage to property, etc.);
- Amendments to the law on criminal procedure to implement the IT-specific instruments;
- Creation of new guidelines on cyber-related cooperation with regard to ECOWAS states, the Council of Europe, and cooperation between the state and ECOWAS/Council of Europe/G8 Network.

Source: Mouhamadou, L.O. 2011. Cybercrime, Civil Liberties, and Privacy in the Economic Community of West African States . 21st Annual Computers, Freedom and Privacy Conference 2011.

Nonetheless, analysis of responses to the Study questionnaire alone shows that membership of a multilateral instrument correlates with a perception of increased *sufficiency* of national cybercrime criminal and procedural law. Figure 3.9 demonstrates that responding countries that were *not* party to a multilateral cybercrime instrument more frequently reported that national cybercrime criminalization and procedural laws were 'not sufficient.'[106]

---

101 Cassese, A., 2005. *International Law*. Oxford: Oxford University Press, p.220-221.

102 Klip, A., 2006. European Integration and Harmonisation and Criminal Law. *In:* Curtin, D.M. et al. European integration and law: four contributions on the interplay between European integration and European and national law to celebrate the 25th anniversary of Maastricht University's Faculty of Law. For general discussion, see Legrand, P., 1997. The Impossibility of 'Legal Transplants, *Maastricht Journal of European and Comparative Law*, (4):111-124.

103 European Commission. 2008. *Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems*. COM (2008) 448 final, Brussels, 14 July 2008. It should be noted that the implementation analysis was carried out only for 20 out of 27 Member States of the European Union, and was based only on formal analysis of the information submitted by Member States.

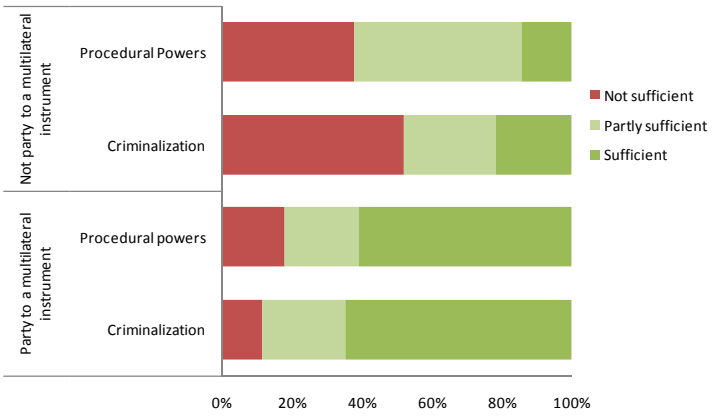
104 Calderoni, F., 2010. The European legal framework on cybercrime: striving for an effective implementation. *Crime, Law and Social Change*, 54(5):339-357.

105 The Mechanism for the Review of Implementation of the United Nations Convention against Corruption, for example, involves a detailed terms of reference for the review process, as well as guidelines for governmental experts and the secretariat in the conduct of country reviews. See http://www.unodc.org/documents/treaties/UNCAC/Publications/ReviewMechanism-BasicDocuments/Mechanism_for_the_Review_of_Implementation_-_Basic_Documents_-_E.pdf

106 Study cybercrime questionnaire. Q19. Figure 3.9 is calculated for the following signed or ratified instruments: Council of Europe Cybercrime Convention, League of Arab States Convention, Commonwealth of Independent States Agreement, and Shanghai Cooperation Organization Agreement.

While a relationship between 'sufficiency' of legislation and 'instrument membership' can be demonstrated, responses to the study did not reveal a clear pattern between 'perceived harmonization' and 'instrument membership.' As noted above, while countries in Europe, for example, perceive high levels of harmonization 'with multilateral instruments,' this does not always translate into perceived high levels of harmonization of national legislation within the region.[107]

Figure 3.9: Impact of multilateral instruments on perceived sufficiency of legislation



Source: Study cybercrime questionnaire. Q19. (n=42)

Similarly, calculations based on the two respondent groups above ('instrument' and 'no instrument') do not reveal significant differences in perceived levels of harmonization with other countries, or within respective regions.[108] Nonetheless, multilateral instruments are usually *inherently* intended to play a role in harmonization and it is possible that responses to the questionnaire also reflect differences in perceptions as to what constitutes 'harmonization' in the first place. In this respect, a number of countries reported positive experiences of implementation of multilateral instruments. In reporting on harmonization successes, for example, many responding countries noted a positive experience in incorporating provisions from instruments such as the Council of Europe Cybercrime Convention into national law.[109]

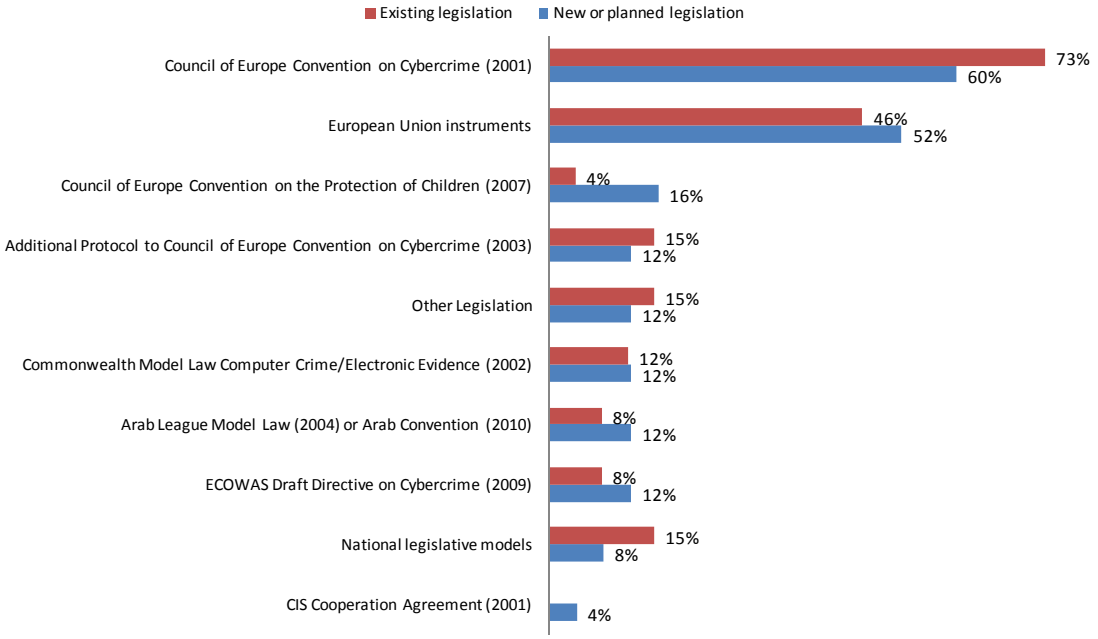
Indirect influence

In addition to formal instrument membership and implementation, multilateral cybercrime instruments have also influenced national laws *indirectly*. This includes through use as a model by non-States parties, or via the influence of legislation of States parties on other countries. Countries may use *more than one* instrument to draft national legislation and a number of countries reported that this was the case.[110] One country in Western Africa, for example, noted use of the Commonwealth Model Law, the Council of Europe Cybercrime Convention, and the ECOWAS Draft Directive. Another country in Western Asia reported use of both the League of Arab States Model Law, and national legislative provisions from other countries in the region.[111] In addition, as noted previously, multilateral instruments themselves include a significant amount of cross-fertilization between the texts. The Commonwealth Model Law and the EU Decision on Attacks against Information Systems, for example, were drafted closely in line with the Council of Europe Cybercrime Convention.

---

107 See above, Section 3.2 Divergence and harmonization of laws, Harmonization of laws.
108 Study cybercrime questionnaire. Q17.
109 Study cybercrime questionnaire. Q16.
110 Study cybercrime questionnaire. Q12 and Q14.
111 *Ibid.*

Figure 3.10: Cross-national instruments used to draft or develop planned or existing national cybercrime legislation



Source: Study cybercrime questionnaire. Q12 and Q14. (n=26,25; r=51, 50)

The complexity of direct implementation of instruments, indirect influence, and their combination, is reflected in aggregate results from the Study questionnaire. During information gathering for the Study, countries were asked which international or regional instruments were used to draft or develop existing and new or planned legislation.[112] A comparatively low number of countries responded to the question.[113] Figure 3.10 shows, however, that the Council of Europe Convention, its Protocol, and instruments closely based on the Council of Europe Convention, such as European Union instruments, were most widely used for the development of cybercrime legislation. Altogether, multilateral instruments from other international or regional 'clusters'[114] – such as the League of Arab States and African instruments – or other national legislation, were used in around half as many countries.

It should be noted that this assessment is based on country responses and not on an examination of the content of national laws.[115] This is appropriate insofar as, in general, it is nearly impossible to identify – merely by analysis of legislative provisions – exactly which instruments were used to draft legislation. Only when the approach to the criminalisation of a particular offence suggested by a specific international framework shows some recognisable differences to all of the other instruments, is it possible to 'trace' any influence. For example, the Commonwealth of Independent States Agreement[116] attaches additional elements to illegal access (effects on data) and criminalizes the distribution of computer viruses in a specific way. Provisions following this

112 *Ibid.*

113 The regional distribution was as follows: regarding existing legislation: Europe 13; Asia & Oceania 7; Americas 5; Africa 5; regarding new or planned legislation: Europe 7; Asia & Oceania 10; Americas 5; Africa 6.

114 See above, Section 3.3 Overview of international and regional instruments.

115 Note that in Chapters Four (Criminalization) and Five (Law enforcement and investigations) of this Study, some results are presented based on primary source legislation analysis.

116 Commonwealth of Independent States Agreement, Art. 3(1)(a): The illegal accessing of computer information protected by the law, where such act results in the destruction, blocking, modification or copying of information or in the disruption of the functioning of the computer, the computer system or related networks.

approach can be found by analysing the content of legal provisions in several countries in Eastern Europe and Western Asia.[117]

The overall potential for success of harmonization and implementation of international law into national legislation is determined, to a large extent, by the degree to which countries are able to translate international standards into national systems. This needs to occur, not only from the legal perspective, but also in a socio-political environment in which there is a high degree of support for, and commitment to, the necessary legislative reforms. This is most likely when countries are able to maintain legal traditions while still meeting the international obligations they have chosen to assume.

One responding country in Western Asia, for example highlighted the necessity of taking into account '*society, in terms of customs and traditions*.'[118] One country in Western Africa and a country in the Americas also pointed out the good practice of using '*stakeholder consultations*' to ensure the maintaining of national legal traditions. In other cases, countries may not yet perceive a need for strengthening cybercrime law. One country in Southern Africa, for instance, noted that since '*the development of ICT infrastructure is still poor, cybercrime legislation was not considered a pressing need.*'[119]

Ultimately, however, the use of both binding and non-binding international and regional instruments has significant potential for positive progress towards greater sufficiency and harmonization of national laws – and, in the long run, enhanced international cooperation against a global challenge. Chapters Four (Criminalization), Five (Law enforcement and investigations) and Eight (Prevention) examine further both convergences and divergences in these individual areas.

117 See Chapter Four (Criminalization).
118 Study cybercrime questionnaire. Q16.
119 *Ibid.*

CHAPTER FOUR: CRIMINALIZATION

This Chapter provides a comparative analysis of cybercrime offences found in national and international law. It demonstrates a certain baseline consensus on the need for criminalization of a set of cybercrime acts. However, closer examination of offence elements shows divergence between countries and multilateral cybercrime instruments. The Chapter also demonstrates the 'sword and shield' effect of international human rights law on cybercrime criminalization.

4.1 Criminalization overview

KEY RESULTS:

- Countries report widespread criminalization of the 14 cybercrime acts contained in the Study questionnaire, with the primary exception of spam offences and, to some extent, offences concerning computer misuse tools, racism and xenophobia, and online solicitation or 'grooming' of children
- This reflects a certain baseline consensus on culpable cybercrime conduct
- 'Core' cybercrime acts against the confidentiality, integrity and accessibility of computer systems are criminalized in many countries using cyber-specific offences
- Computer-related acts, such as those involving breach of privacy, fraud or forgery, and identity offences, are more often criminalized using general offences
- 80 per cent of countries in Europe report sufficient criminalization of cybercrime acts
- In other regions of the world, up to 60 per cent of countries report that criminalization of cybercrime acts is insufficient

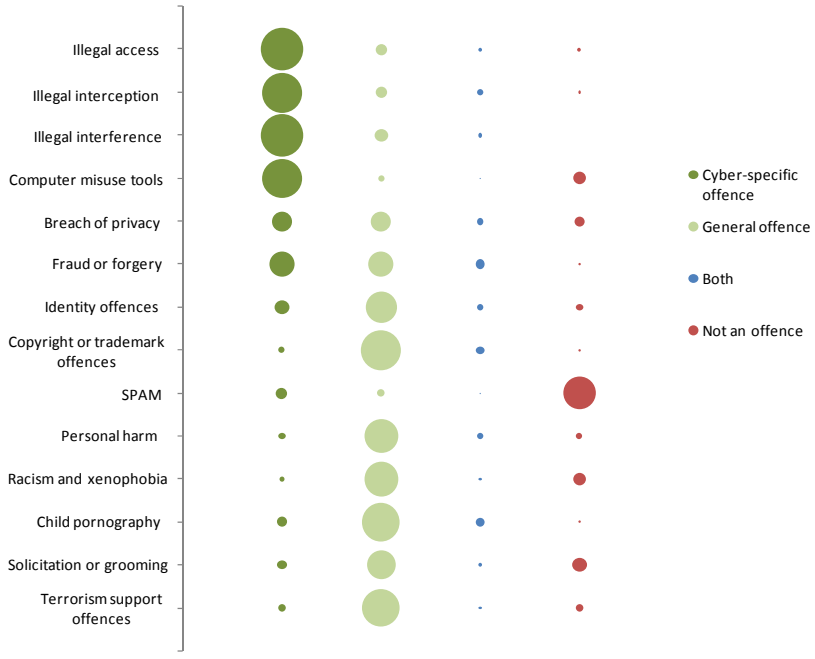
The aim of this Chapter is to provide a comparative analysis of cybercrime offences found in national law. An understanding of criminalization approaches used, and differences between national criminal laws in the area of cybercrime, is important for three reasons. Firstly, as discussed, in Chapter Three (Legislation and frameworks), criminalization *gaps* in any country can create offender havens with the potential to affect other countries globally. Secondly, criminalization *differences* introduce challenges for effective international cooperation in criminal matters involving cybercrime – in particular, as regards the principle of dual criminality. Thirdly, a comparative analysis of cybercrime offences is able to explore *good practice* that states may use in the development of national laws, in accordance with emerging international standards in this area. Following a general overview of cybercrime criminalization, the Chapter examines the specific ways in which states structure a number of cybercrime offences in national laws. It concludes with a discussion of the impact of international human rights law on cybercrime criminalization.

Cyber-specific and general offences

Individual cybercrime acts – such as those identified in Chapter One (Connectivity and cybercrime) – may be addressed by states in a number of ways. Some acts may not be a criminal offence at all in national law. Where acts are a criminal offence, this may be under a general (non-cyber-specific law), or a specialized cyber-specific offence. Other acts may not be a criminal offence, but addressed by administrative sanctions, or subject to civil remedies. A number of responding countries indicated that administrative sanctions were used for a range of acts that were not considered a *criminal* offence, including copyright and trademark offences, sending or controlling sending of spam, acts involving breach of privacy, and the production, distribution or possession of computer misuse tools.[1] This Chapter does not examine the use of administrative sanctions or civil remedies, but rather focuses on *criminalization*. The Chapter begins with an overview of the *extent* of criminalization of different cybercrime acts, before focusing on the *content* of national provisions.

Figure 4.1 provides a broad overview of the extent of criminalization for the 14 cybercrime act categories, as reported in more than 60 country responses to the Study questionnaire. Responses demonstrate widespread criminalization of the 14 acts, with the primary exception of spam offences and, to some extent, offences concerning computer misuse tools, racism and xenophobia, and online solicitation or 'grooming' of children.[2] This reflects a certain baseline consensus on culpable cybercrime conduct. As noted in Chapter One (Connectivity and cybercrime), countries reported few additional crimes not mentioned in the questionnaire. These mostly concerned computer content, including criminalization of obscene material, online gambling, and online illicit markets, such as in drugs and persons. The use of criminal law to regulate computer and internet content in particular, is discussed later in this Chapter within the context of the impact of international human rights law on criminalization.

Figure 4.1: National approaches to criminalization of cybercrime acts



Source: Study cybercrime questionnaire. Q25-38. (n=61)

Figure 4.1 also shows the clear pattern of use of cyber-specific law for 'core' cybercrime offences involving acts against the confidentiality, integrity and accessibility of computer systems. Cyber-specific offences are less commonly used for other cybercrime acts, such as computer-related acts for personal or financial gain or harm, or computer content-related acts. In contrast, the role of *general* criminal offences becomes significant for these latter categories. Notably, some countries report using general offences even for core cybercrime acts, such as illegal access to

1 Study cybercrime questionnaire. Q25-39.
2 *Ibid.*

a computer system or data, and illegal data interference or system damage. The distribution between cyber-specific offences and general offences is examined in detail for selected acts later in this Chapter.

The wide distribution between cyber-specific and general offences supports the approach taken at the international level to characterize the place of 'cybercrime' within the spectrum of 'crime' as a whole. Initial work undertaken on an 'International Crime Classification Framework' mandated by the United Nations Economic and Social Council,[3] for example, classifies some cybercrime acts at the 'vertical' level (as specific, mutually-exclusive offence categories), but also envisages cybercrime acts at the 'horizontal' level, as an 'attribute' of traditional crimes that involve a computer element.[4]

In addition to examining the cyber-specific or general nature of cybercrime offences, it is also important to consider the *general* criminal law. Cybercrime offences in national laws are not applied or interpreted by the criminal justice system in isolation, but rather with reference to rules that apply to all offences, such as rules on complicity, attempt, omission, state of mind, and legal defences. When it comes to 'state of mind', in particular, any comparative law exercise must be carried out with caution. Different legal systems use a range of different concepts and definitions. The same terms in different legal systems may even have different meanings. Legal systems may distinguish between 'will' and 'knowledge', or define a range of mental states, such as 'purposefully', 'with knowledge', 'recklessly', and 'negligently'.[5] In all legal systems, however, two general poles of 'intentional' and 'non-intentional' culpable conduct can be discerned.[6]

Such distinctions are important when it comes to cybercrime offences. A number of international and regional instruments, for example, specify that conduct shall be established as a criminal offence '*when committed intentionally*.'[7] Other instruments allow that criminal offences may be committed recklessly. The Draft African Union Convention, for example, states that each Member state of the African Union shall take the necessary legislative measures to set up '*as a penal offence*' the fact '*even out of negligence*' of processing of personal data, without following the necessary rules for data processing.[8] In some African countries, the mental element of 'fraudulently' is also commonly used in penal law. The ECOWAS Draft Directive, for example, contains articles such as the '*fraudulent interception of computer data*' and '*fraudulent access to computer systems*.'[9] In this context, the level of intent required might be considered equivalent to a form of 'dishonest' intent – more than the general standard of 'intentionally', but less than a specific intent to obtain monies, goods or services, by deceit or falsehood.

Due to the potential broad reach of some cybercrime offences, such as illegal access to computer data, it is important that the mental element of cybercrime acts is clearly defined in law. This may be in the offence itself, or through the general criminal law. Where possible, the legislative analysis in this Chapter attempts to identify similarities and differences in offence intent elements.

---

3 United Nations Economic and Social Council, 2012. Resolution 2012/18. *Improving the quality and availability of statistics on crime and criminal justice for policy development.*

4 See Centre of Excellence in Statistical Information on Government, Crime, Victimization and Justice, 2012. *Report on the Consultation meeting for the International Crime Classification Framework.* 17-19 October 2012, Mexico City.

5 For the categories of the mental element in European continental law countries, see, for example, Roxin, C., 2010. *Strafrecht AT I.* 4th ed. Munich. pp.436 et seq. and 1062 et seq. (Germany); Picotti, L., 1993. *Il dolo specific.* Milan (Italy). For the categories of the mental element in common law countries, see Dressler, J., 2012. *Understanding Criminal Law.* 6th ed. pp.117–144 (United States); Ashworth, A., 2009. *Principles of Criminal Law.* 6th ed. pp.75, 154-156, 170-191 (United Kingdom).

6 'Intentionally' includes especially purposely and knowingly. 'Non-intentionally' ranges from recklessness to gross and simple negligence.

7 See, for example, Council of Europe Cybercrime Convention, Arts. 2-9.

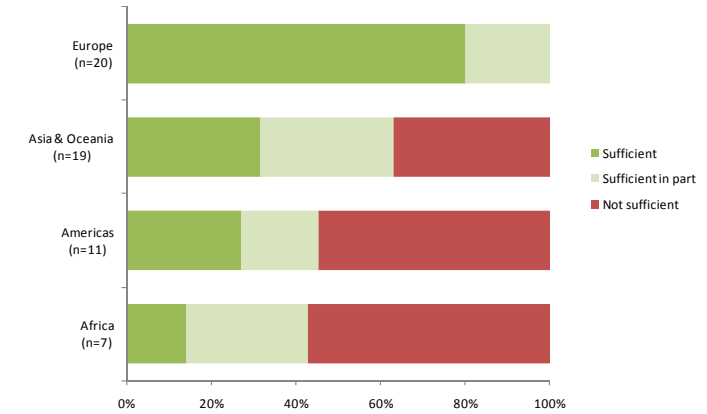
8 Draft African Union Convention, Part IV, Section 3, Art III-29.

9 ECOWAS Draft Directive, Arts. 2-11.

Sufficiency of criminal laws for cybercrime

In addition to diversity of criminal legislation approach, countries also show differences in perceived 'sufficiency' of their cybercrime criminalization frameworks. Around 80 per cent of countries from Europe that responded to the Study questionnaire reported that their criminal laws for cybercrime were sufficient, with the remainder reporting that they were sufficient 'in part.' In contrast, in other regions of the world, up to 60 per cent of countries reported that their criminal law frameworks were 'not sufficient.'

Figure 4.2: Sufficiency of national law for criminalization



Source: Study cybercrime questionnaire. Q41. (n=57)

When asked about the main *gaps* in cybercrime criminal law, many countries referred either to the fact that criminal laws, in general, were not well suited to cybercrime, or to the absence of offences for particular cyber-conduct. One country in Africa, for example, reported that '*There are no offences of a cyber- or information-related nature.*' Another, in Western Asia, referred to the general problem that '*The forms and essential elements of natural crime mentioned in the Criminal Code cannot be applied to electronic crimes.*' A country in Southern Asia also noted that '*We need to have detailed and specific law[s] that should make different aspects of cyber-related acts an offence. Unfortunately, we are waiting for one such law that has not yet been approved.*'[10] With respect to specific conduct gaps, a country in Western Asia highlighted that '*There is a legal gap regarding the criminalization of data theft for economic gain.*' A country in the Caribbean noted that '*There are no specific laws dealing with sending of spam, computer-related acts involving racism and xenophobia, discrimination, cyber bullying and identity theft etc.,*' and a country in South-Eastern Asia highlighted that '*some specific cybercrimes are currently not criminal offences such as denial of service (DOS) attacks, and spam.*' Many countries reported requiring legislation to deal with highly specific cyber-conduct. One country in Europe, for example, reported that '*currently* [*we*] *do not criminalize botnets, spoofing and grooming.*' Another in South-Eastern Asia noted that '*currently, online harassment, cyber-stalking, and some identity-related crimes are not adequately addressed.*'[11]

Conversely, countries also reported many strengths and good practices in the criminalization of cybercrime acts. A country in North America, for example, indicated that it was good practice to have '*Broad coverage of cybercrime acts in technologically neutral language.*' One country in South-Eastern Asia reported that a mixed approach of cyber-specific and general offences was effective, as '*computer integrity crimes are comprehensively covered by the Computer Misuse Act* [*and*] *most other forms of cybercrime are also addressed to a large extent, though by non-cyber specific laws.*' A country in Oceania highlighted a need for '*wide coverage of acts of cybercrime*' and the importance of deterrence through '*strong penalties.*'[12]

10 Study cybercrime questionnaire. Q41.
11 *Ibid.*
12 *Ibid.*

4.2 Analysis of specific offences

KEY RESULTS:

- While wide consensus exists regarding broad areas of criminalization, detailed analysis of the provisions in source legislation reveals divergent approaches that are apparent both at national and, in some cases, international level
- The detail of cybercrime offences matters. Differences in the elements of offences can create challenges to the equivalence of offences in different countries for the purposes of international cooperation. Small changes in offence elements, such as extension to 'non-intentional' states of mind can risk over-criminalization
- Offences involving illegal access to computer systems and data differ with respect to the object of the offence (data, system, or information) and regarding the criminalization of 'mere' access or the requirement for the circumvention of security measures or further intent, such as to cause loss or damage
- Criminalization of illegal interception differs by virtue of whether the offence is restricted to non-public data transmissions or not, and concerning whether the crime is restricted to interception 'by technical means'
- Differences exist between countries as to the acts constituting computer system or data interference. Most countries require interference to be intentional, but some include reckless interference
- Not all countries criminalize computer misuse tools. For those that do, differences arise regarding whether the offence covers use of software tools and/or computer access codes. Differences also exist concerning whether laws require that the tool itself was designed for the commission of an offence, and/or whether the perpetrator intended to use it for an offence
- National laws on child pornography use a range of terminologies but only in around one-third of countries do they include simulated material. The majority of countries define child pornography with reference to the age of 18 years but some countries use lower age limits. Around two-thirds of countries include criminalization of possession of child pornography

This section of the Chapter contains a detailed analysis of the provisions of selected cybercrime offences in national laws with a view to identifying both divergences between countries that may present a challenge to harmonization of cybercrime legislation, and common elements of offences that could be considered good practice. The analysis is based on two sources: (i) country responses to the Study questionnaire; and (ii) analysis of primary source legislation for a wider group of almost 100 countries.[13] Throughout the section, the source used is indicated at each stage.[14] In general, country questionnaire responses are used to assess the *existence* of an offence covering a particular cybercrime act. For those countries that criminalize the act, primary source legislation analysis is then used to examine the *contents* of the offence in national law, using the method of

[13] Primary source legislation was analysed for 97 countries, including 56 that responded to the questionnaire. The regional distribution is as follows: Africa (15), Americas (22), Asia (24), Europe (30), and Oceania (6). It was not possible to include 13 countries that responded to the questionnaire in the primary source legislation analysis due to insufficient information on relevant legislation provided in the questionnaire.

[14] Source attributions are: (i) 'Study cybercrime questionnaire'; and (ii) 'UNODC legislation analysis'. It should be noted that analysis of primary source legislation is unable to easily take account of legal interactions between specific provisions and other general parts of criminal law, or of the effect of judicial decisions or other interpretative law that affects the reading of the original legislative provision.

'functional' comparative law.[15] For primary source legislation analysis, legislation for each particular cybercrime act was not available from all countries. Thus, numbers of countries included in this part of the analysis vary depending upon the cybercrime offence examined.[16]

Illegal access to a computer system

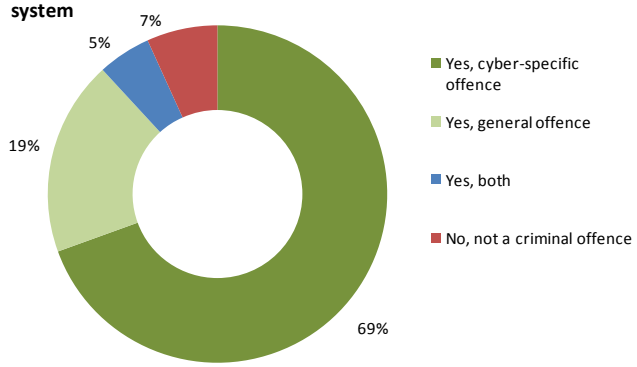
The act of accessing a computer system without proper authorization has existed since the early days of the development of information technologies.[17] Illegal access threatens interests such as the integrity of computer systems. The legal interest is infringed not only when a person without authorization alters or 'steals' data in a computer system belonging to another, but also when a perpetrator merely 'looks around' in the computer system. The latter infringes upon the confidentiality of the data, and considerable actions on the part of the victim may be required to check the integrity or status of the system. 'Pure' or 'mere' illegal access to a computer system does not require that the offender accesses system files or other stored data. Criminalization of illegal access thus represents an important deterrent to many other subsequent acts against the confidentiality, integrity and availability of computer systems or data, and other computer-related offences, such as identity theft and computer-related fraud or forgery.[18]

Illegal access: Council of Europe Cybercrime Convention

Article 2 – Illegal Access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Figure 4.3: Criminalization of illegal access to a computer system



Source: Study cybercrime questionnaire. Q25. (n=59)

As a consequence, eleven multilateral instruments require the adoption of provisions criminalizing illegal access to computer systems or data.[19] Legislation on the national level well reflects this requirement. Figure 4.3 shows that about 70 per cent of responding countries to the Study questionnaire reported the existence of the cyber-specific offence of illegal access to a computer system.[20] In addition, about 20 per cent of responding countries reported that the act was covered by general provisions of criminal law. Very few countries, only 7 per cent, do not criminalize illegal access to a computer system at all.

---

15 For details of the methodology of comparative criminal law, see Sieber, U., 2006. Strafrechtsvergleichung im Wandel. *In:* Sieber, U., Albrecht, H.J. *Strafrechtsvergleichung und Kriminologie unter einem Dach.* Berlin: Duncker & Humblot, pp.78 and 111-130.

16 A maximum number of 90 countries were analysed (for illegal access provisons), and a minimum number of 70 were analysed (for child pornography and computer misuse tool provisions).

17 See Kabay, M., 2009. History of Computer Crime. *In:* Bosworth, S., Kabay, M.E. and Whyne, E., *Computer Security Handbook.* 5th ed. New York: Wiley; Sieber, U., 1986. *The International Handbook of Computer Crime.* Chichester: John Wiley & Sons, pp.86-90.

18 See Council of Europe, 2001. *Explanatory Report to Council of Europe Cybercrime Convention*, ETS No. 185, para. 44: *'Illegal access covers the basic offense of dangerous threats to and attacks against the security (i.e., the confidentiality, integrity and availability) of computer systems and data.'*

19 Draft African Union Convention, Arts. III-15, III-16; COMESA Draft Model Bill, Arts. 18, 19; Commonwealth Model Law, Art. 5; Council of Europe Cybercrime Convention, Art. 2; ECOWAS Draft Directive, Art. 2; EU Decision on Attacks against Information Systems, Art. 2(1); EU Directive Proposal on Attacks against Information Systems, Art. 3; ITU/CARICOM/CTU Model Legislative Texts, Art. 4; League of Arab States Convention, Art. 6; League of Arab States Model Law, Art. 3, 5, 15, 22; Commonwealth of Independent States Agreement, Art. 3(1)(a).

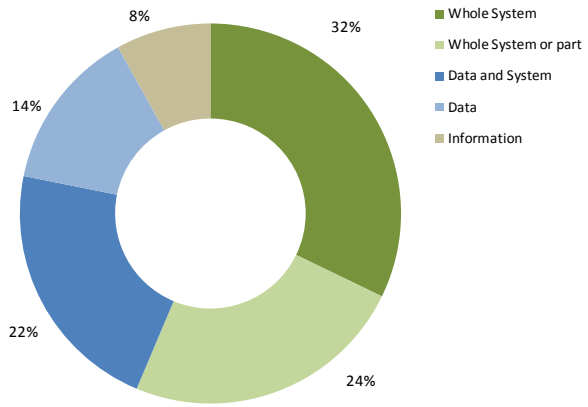
20 Study cybercrime questionnaire. Q25.

Primary source legislation analysis of illegal access provisions for some 90 countries shows cross-national differences with regard to the object of crime, the acts covered and the mental element.

Offence object - All international and regional cybercrime instruments provide for criminalization of illegal access to the *whole* or *part* of a computer system. Only around 55 per cent of the countries included in the primary source legislation analysis, however, follow this approach.

Figure 4.4 demonstrates that some national laws limit the object of illegal access to *data* or *information* instead of a system, or criminalize access to *both* data and system, sometimes in different provisions. Some national provisions go even further in limiting the approach. Several countries in Western Asia and Eastern Europe, for example, criminalize illegal access to '*information protected by law*.'

Figure 4.4: Objects of illegal access



Source: UNODC legislation review. (n=87)

Acts covered – Criminalization of 'mere' illegal access, or the requirement for further intent or acts, represents another point of divergence. All international instruments provide for the option of criminalization of *mere* unauthorized access to a computer system. Some instruments, however, allow for further conditions. The Council of Europe Cybercrime Convention[21] and the ITU/CARICOM/CTU Model Legislative Texts,[22] for example, provide countries with the possibility of attaching additional conditions – such as 'bypassing security' or 'dishonest intent'. The EU Decision on Attacks against Information Systems gives Member states an opportunity to avoid criminalization of minor cases.[23] The Commonwealth of Independent States Agreement requires criminalization of illegal access if it results in '*destruction, blocking, modification or copying of information or the disruption of the functioning of the computer, the computer system or related networks.*'[24]

Such conditions enable states to adopt narrower legislation on illegal access. Indeed, consensus is not universal on the desirability of criminalization of mere illegal access to non-protected systems.[25] On the other hand, some conditions provided by international approaches, especially those that include requirements for additional acts, may lead to challenges in distinguishing illegal access from *subsequent* offences – with possible confusion of boundaries between illegal access and offences such as data interference or data espionage.

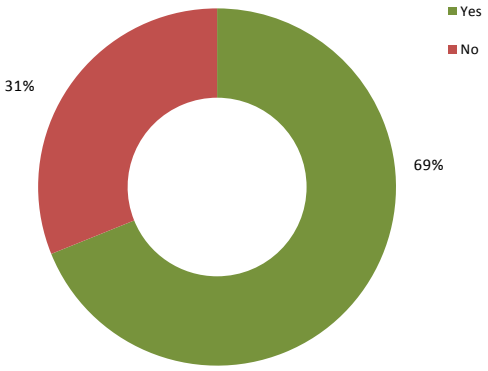
Illegal access: National example from a country in Southern Europe

Whoever, without legal permission or authorization from the owner or holder of the right over the full system, or part thereof, accesses a computer system, shall be punishable by a term of imprisonment up to ___ year or by fine up to ____.

21 Council of Europe Cybercrime Convention, Art. 2.
22 ITU/CARICOM/CTU Model Legislative Texts, Art. 5.
23 EU Decision on Attacks against Information Systems, Art. 2.
24 Commonwealth of Independent States Agreement, Art. 3(1)(a).
25 See, for example, Sieber, U., 1985. *Informationstechnologie und Strafrechtsreform.* Cologne: Carl Heymanns Verlag, p.49.

Figure 4.5 shows that, of those countries that criminalize illegal access, around 70 per cent criminalize mere illegal access. The remaining 30 per cent require additional conditions for the act to constitute a crime. There is no clear regional pattern to this result. A few countries require either '*infringement of security measures*' or additional intent, such as the '*intent to commit another crime.*' Some national laws limit illegal access only to cases of '*grave violations*' or '*serious crimes,*' as in the case of one country in Oceania.[26] In addition, some national statutes criminalize illegal access only where data are '*copied*', '*blocked*', '*stolen*', '*modified*' or '*deleted*', or if illegal access is committed '*in connection with*' system interference. In some countries, this leads to the criminalization of illegal access as one of the *elements* of data and system *interference* offences. For example, one country in Eastern Europe criminalizes the act of '*interference with data and systems*' only if committed '*in conjunction*' with unauthorized access to a computer system. This has the effect of limiting criminalization of data interference to the cases where illegal access is the first step in committing the offence against data and systems.

Figure 4.5: Criminalization of mere illegal access



Source: UNODC legislation review. (n=90)

State of mind - All multilateral instruments require the crime of illegal access to be committed intentionally or, in the case of two instruments, '*fraudulently.*'[27] However, the definition of what constitutes 'intent' is usually left to the implementing country. For example, the Explanatory Report to the Council of Europe Cybercrime Convention states explicitly that the exact meaning of 'intentionally' should be '*left to national interpretation.*'[28] In this respect, as discussed above, the exact state of mind considered to constitute 'intentionality' differs between many national legal systems – depending upon both special and general criminal law.[29]

Analysis of primary source legislation, however, shows that, for those illegal access provisions that specifically mention state of mind, the mental elements of '*intentionally*', '*knowingly*', '*wilfully*', and '*fraudulently'* are used – indicating that some form of intentionality is most usually required for the offence. In only two countries included in the analysis, situated in the Caribbean and Oceania, can illegal access be committed '*recklessly.*'

Aggravating circumstances – Four multilateral cybercrime instruments include aggravating circumstances in provisions on illegal access. The League of Arab States Model Law provides for aggravated penalties for illegal access committed '*with intention of nullifying, deleting, destroying, disclosing, damaging, changing or re-disseminating personal data or information'* (Art. 3), or for illegal access committed by the offender '*in the course of or because of the discharge of his functions or has facilitated commission of the offences by a third party*' (Art. 5). The League of Arab States Convention provides for aggravating circumstances if access leads to the '*obliteration, modification, distortion, duplication, removal or destruction of*

---

26 This country limits criminalization to acts committed with the intent to commit, or facilitate the commission of, a serious offence against a law by access. A serious offence is further defined as an offence punishable with lifetime imprisonment or at least for a period of more than five years.

27 Draft African Union Convention, Arts. III-15, III-16; ECOWAS Draft Directive, Arts. 2, 3.

28 Council of Europe, 2001. *Explanatory Report to Council of Europe Cybercrime Convention*, ETS No. 185, para. 39: *'All the offences contained in the Convention must be committed 'intentionally' for criminal liability to apply. In certain cases an additional specific intentional element forms part of the offence. For instance, in Article 8 on computer-related fraud, the intent to procure an economic benefit is a constituent element of the offence. The drafters of the Convention agreed that the exact meaning of 'intentionally' should be left to national interpretation.'*

29 See, for example, LaFave, R.W., 2000. *Criminal Law*. 3rd ed. St. Paul: MN. pp. 224-234; Fletcher, G., 1998. *Basic Concepts of Criminal Law*. Oxford University Press, pp.99-100, 111-129; Fletcher, G., 1971. The Theory of Criminal Negligence: A Comparative Analysis. *University of Pennsylvania Law Review*, 119(3):401-403.

saved data, electronic instruments and systems and communication networks, and damages to the users and beneficiaries, or to the acquirement of secret government information' (Art. 6). The COMESA Draft Model Bill has additional provisions criminalizing illegal access to '*government computers*' or '*computer systems used for critical infrastructure operations*' (Art. 19). The EU Directive Proposal on Attacks against Information Systems (Art. 10) introduces the requirement of aggravated penalties for crimes of illegal access committed: (i) within the framework of a '*criminal organisation*'; (ii) through the use of a '*tool designed to launch attacks affecting a significant number of information systems*' or attacks causing considerable damage, such as disrupted system services, financial cost, or loss of personal data; or (iii) by '*concealing the real identity*' of the perpetrator and causing prejudice to the rightful identity owner.

At the national level, many countries that criminalize mere illegal access have also created aggravating circumstances that attract more severe sanctions. Such circumstances vary significantly from country to country. Those identified include:

- Commission of the act with illegal financial or detrimental intent;
- Interfering with the functioning of a computer system;
- Suppressing or altering data;
- Copying, using, disclosing, or any other violation of computer data or programmes;
- Accessing a third computer;
- Causing considerable damage;
- Creating public disorder;
- Facilitating or supporting terrorism;
- Committing the act as a member of an organized group;
- Combining the act with violent behaviour.

As discussed above, many such circumstances present overlap with other possible, separate, offences, such as illegal data interference or system damage. The most common aggravating circumstance seen during primary source legislation review, however, was the involvement of computers critical to the functioning of infrastructure such as banking, telecommunications, health services, public services or government computers. More than half of the national laws examined provided special protection by way of increased penalties for illegal access to computers run by state authorities, or that could be linked to the functioning of critical infrastructure.

Illegal remaining in a computer system

Two multilateral instruments cover not only illegal access to a computer system, but also '*remaining in*' a system without the right to do so after authorisation has expired.[30] The ITU/CARICOM/CTU Model Legislative Texts give countries the possibility of not criminalizing mere unauthorized remaining in the system, provided that other effective remedies are available. The ECOWAS Draft Directive, on the other hand, requires criminalization of '*fraudulently*' remaining in a computer system.

Illegal remaining: ECOWAS Draft Directive

Article 3 – Fraudulently remaining in a computer system
The act by which a person fraudulently remains or attempts to remain within the whole or part of a computer system.

These divergences are reflected in the national legislation. Some laws incorporate the concept of illegal remaining into illegal access provisions, while others criminalize it separately. More

[30] ECOWAS Draft Directive, Art. 3; ITU/CARICOM/CTU Model Legislative Texts, Art. 5.

commonly, however, illegal remaining is not specifically criminalized at all. From the countries included in the primary source legislation analysis, only nine countries, distributed across regions, criminalized illegal remaining. Eight do so through incorporation into an illegal access provision, while one does so in a separate provision.

Illegal interception of computer data

Criminalization of illegal interception extends protection of the integrity and confidentiality of computer data from data residing in a system to all transmitted data. A primary concern behind prohibition of the interception of computer data in transmission is the breach of confidentiality in private communications.[31]

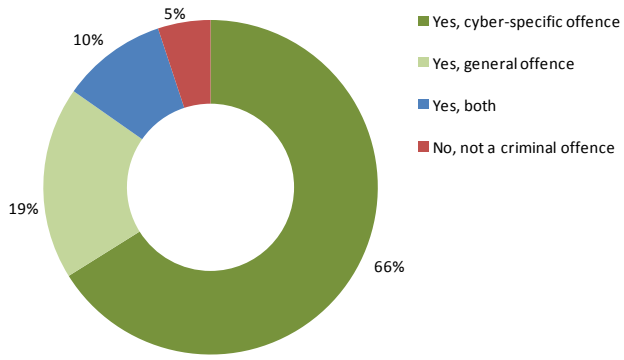
Illegal interception: ECOWAS Draft Directive

Article 6 – Fraudulent interception of computer data
The act by which a person fraudulently intercepts or attempts to intercept computerized data during their non-public transmission to, from or within a computer system through technical means.

Nine international instruments include specific provisions criminalizing interception of computer data.[32] At the national level, while many countries have specific offences covering interception of computer data, others apply existing laws, including prohibitions on the interception of communications in general. One reason for this is the fact that interception of computer data can be viewed from either, or both, of the perspectives of integrity of data, or the protection of privacy.

The Study cybercrime questionnaire asked about illegal interception of computer data in the context of interception, access or acquisition of computer data. Thus the Study did not collect direct information on illegal interception separately. Nonetheless, Figure 4.6 shows that 85 per cent of responding countries have provisions criminalizing illegal interception, access to, or acquisition of computer data. In just over 65 per cent of countries this is by way of a cyber-specific offence. For those countries that have a cyber-specific offence of illegal interception, analysis of primary source legislation shows differences between the *object* of the offence and the *acts* covered.

Figure 4.6: Criminalization of illegal access, interception or acquisition of computer data



Source: Study cybercrime questionnaire. Q26. (n=59)

Offence object – Most multilateral cybercrime instruments define the object of illegal interception as '*non-public*' transmission of computer data, thus limiting the object to 'private' transmissions. This limitation refers to the intended nature of the transmission. For example, a communication that has a private nature but is sent via public Wi-Fi network can be protected for the purposes of illegal interception, even though the transmission goes through a public network.[33] The only document that does not limit criminalization to non-public transmission is the League of

31 Walden, I., 2007. *Computer Crime and Digital Investigations*. Oxford: OUP, p.184.

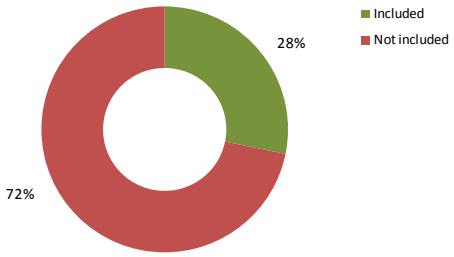
32 Draft African Union Convention (Art. III-23); COMESA Draft Model Bill, Art. 21; Commonwealth Model Law, Art. 8; Council of Europe Cybercrime Convention, Art. 3; ECOWAS Draft Directive, Art. 6; EU Directive Proposal on Attacks against Information Systems, Art. 6; ITU/CARICOM/CTU Model Legislative Texts, Art. 6; League of Arab States Convention, Art. 7; League of Arab States Model Law, Art. 8.

33 See, for example, Council of Europe, 2001. *Explanatory Report to Council of Europe Cybercrime Convention*, ETS No. 185.

Arab States Model Law (Art. 8). Some multilateral instruments, in addition to non-public transmissions, also cover the interception of '*electromagnetic emissions*' – a term used to widen the scope of the offence.[34]

While the vast majority of multilateral instruments limit the application of illegal interception to private transmissions of computer data, analysis of legislation for 78 countries shows that, on the national level, the scope of the offence in many cases is not restricted to non-public data transfers. Figure 4.7 shows that just under 30 per cent of countries examined limit unauthorized interception to private or protected transmissions. In practice, however, due to the broad interpretation of 'non-public', it is likely that this does not significantly broaden the offence scope.

Figure 4.7: Restriction to private/non-public transmissions



Source: UNODC legislation review. (n=78)

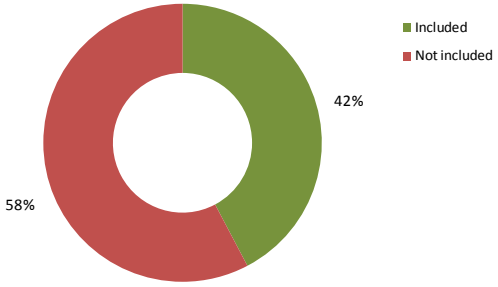
A further issue concerns the concept of 'transmission'. Data can be considered 'in transmission' when they have not reached the final destination – either the system or the intended recipient. Data transmission could be considered to end when the computer *system* of destination is reached. Alternatively, data could be considered as 'in transmission', when stored in the system until the intended recipient obtains access to them. No multilateral instrument provides guidance on the end-point of transmission. The distinction is important with respect to temporary data storage that occurs when computer data are transmitted with the use of protocols operated on a 'store-and-forward' basis.[35]

Illegal interception: National example from a country in the Americas

A person who knowingly and without lawful excuse or justification intercepts by technical means
(a) any transmission to, from or within a computer system that is not available to the public; or
(b) electromagnetic emissions that are carrying computer data from a computer system
is guilty of an offence and is liable on conviction on indictment to a fine of ____ or to imprisonment for a term of ____ years or to both.

Several countries have addressed this issue in national legislation. One country in Oceania, for example, uses a legal provision which excludes '…*communication stored on a highly transitory basis as an integral function of the technology used in its transmission*' from the definition of stored communication. Thus, such data could be included within the scope of the offence of illegal *interception* of computer data.

Figure 4.8: Are technical means included as an element of the illegal interception offence?



Source: UNODC legislation review. (n=78)

Acts covered – Multilateral instruments, with one exception,[36] limit acts of interception to those committed using technical means. As stated in the explanatory report to the Council of Europe Cybercrime Convention, this

[34] Including Commonwealth Model Law; ITU/CARICOM/CTU Model Legislative Texts; EU Directive Proposal on Attacks against Information Systems; and Council of Europe Cybercrime Convention.
[35] Walden, I., 2007. *Computer Crime and Digital Investigations*. Oxford: OUP, p.185.
[36] League of Arab States Convention, Art. 8.

requirement represents a restrictive condition in order to avoid over-criminalization.[37] The limitation, however, is not always reflected in national approaches. Figure 4.8 shows that more than half of the countries for which legislation was analysed, in all regions of the world, do not include technical means as an element of the illegal interception offence.

State of mind – Multilateral instruments usually require that the crime of illegal interception be committed intentionally. The Council of Europe Cybercrime Convention, for instance, provides parties with the possibility to limit the offence of illegal interception to cases committed with dishonest intent. The review of national legislation showed that very few countries require further intent, although some do link interception with the intent to commit further offences. One country in Eastern Europe, for example, criminalizes illegal interception of data only for the purpose of committing specific computer offences. In addition, some countries include additional intent as an aggravating circumstance. Two countries in Western Europe, for instance, provide aggravated penalties for unauthorized interception committed with the intent to achieve financial advantage.

Illegal interference: EU Decision on Attacks against Information Systems

Article 4 – Illegal data interference
Each Member State shall take the necessary measures to ensure that the intentional deletion, damaging, deterioration, alteration, suppression or rendering inaccessible of computer data on an information system is punishable as a criminal offence when committed without right, at least for cases which are not minor.

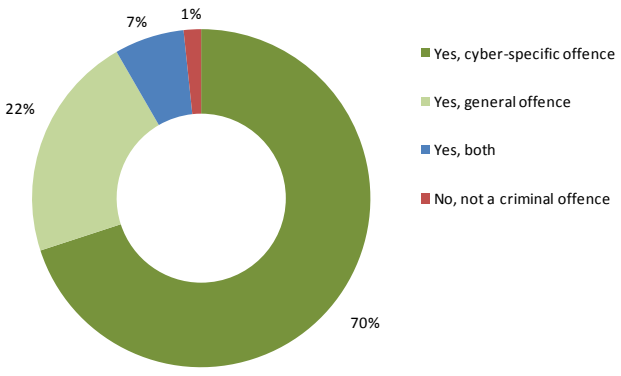
Illegal interference: Council of Europe Cybercrime Convention:

Article 5 – System interference
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Illegal interference with a computer system or computer data

Interference with computer data or systems endangers the integrity and availability of computer data, as well as the proper operation of computer programmes and computer systems. Due to the non-tangible nature of computer data, many national legal systems may not be able to extend traditional criminal law provisions dealing with destruction of physical property to interference with computer data.[38] Most multilateral instruments therefore include specific offences concerning illegal data and/or system interference.

Figure 4.9 : Criminalization of illegal data interference or system damage



Source: Study cybercrime questionnaire. Q27. (n=60)

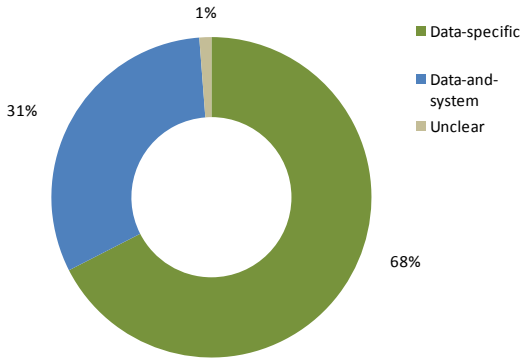
At the national level, Figure 4.9 shows that over 90 per cent of responding countries have a criminal offence covering illegal interference with a computer system or computer data. Seventy per

[37] Council of Europe, 2001. *Explanatory Report to Council of Europe Cybercrime Convention*, ETS No. 185.

[38] Sieber, U., 2008. Mastering complexity in the global cyberspace: The harmonization of computer-related criminal law. *In:* Delmas-Marty, M., Pieth, M. and Sieber, U., (eds.) *Les chemins de l'Harmonisation Pénale/Harmonising Criminal Law. Collection de L'UMR de Droit Comparé de Paris.* Vol. 15. Paris: Société de législation comparée.

cent of these countries report a cyber-specific offence. In 7 per cent of reporting countries, the act is covered by both a cyber-specific and a general offence. Examination of primary source legislation for 83 countries shows differences within national legislation concerning the *object* of the offence, the *state of mind* required, and attached *aggravating circumstances*.

Figure 4.10: Objects of data interference

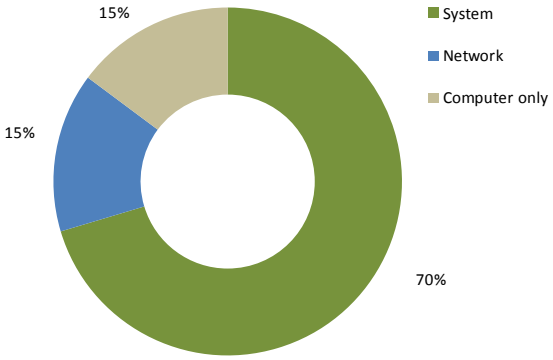


Source: UNODC legislation review. (n=83)

Offence object – Most multilateral instruments require the adoption of *separate* provisions for criminalization of illegal interference with computer *data* and computer *systems.*[39] Only the League of Arab States Model Law combines the two concepts.[40]

For the majority of national legislation examined, data interference and system interference were contained in separate provisions. However, in around 30 per cent of countries examined, the offences are not clearly separated, or data interference is only criminalized when it has an effect on the functioning of a computer system. While this will often be the case in practice, the approach could leave criminalization gaps for interference of computer data alone. Nonetheless, in some countries this may still be covered by general criminal laws. One country in the Americas, for example, makes use of a general provision on destroying or rendering defective 'goods' – in which the definition of 'goods' includes computer data.

Figure 4.11: Objects of system interference



Source: UNODC legislation review. (n=81)

For the *system* element of illegal interference, analysis of available provisions shows that national laws most often cover computer '*systems*'. In 30 per cent of countries, however, the offence was limited either to computer '*networks*' or '*a computer*'. This may limit criminalization by excluding either cases in which a computer that suffers damage is not 'networked,' or cases in which multiple devices, including network routers, suffer interference, such as through a malware or DDoS attack.

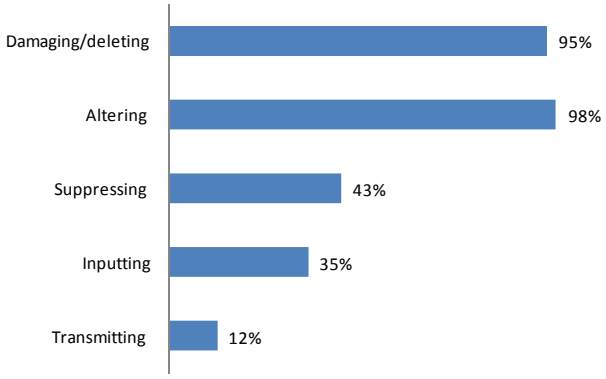
Acts covered – Multilateral instruments cover criminalization of different acts constituting data interference, including not only damage to data but also '*deletion*', '*deterioration*', '*alteration*', '*suppression*', and even '*inputting*' of data, thus protecting data integrity in a broad sense. Figure 4.12 shows that the majority of national laws examined cover damage, or deletion of data, and data alteration. Only 35 per cent of countries included 'inputting' of data in interference provisions. 'Suppressing' data is covered in just over 40 per cent of countries. Only 12 per cent of countries criminalize 'transmission' of data under data interference provisions. It might be expected that 'transmission' of data would be criminalized in countries where data and system interference are

[39] Draft African Union Convention, Arts. III-19, III-20; COMESA Draft Model Bill, Art. 20-b; Commonwealth Model Law, Art. 6; Council of Europe Cybercrime Convention, Art. 4; ECOWAS Draft Directive, Arts. 5, 7; EU Decision on Attacks against Information Systems, Art. 3; EU Directive Proposal on Attacks against Information Systems, Art. 4; ITU/CARICOM/CTU Model Legislative Texts, Art. 7; League of Arab States Convention, Art. 8.

[40] League of Arab States Model Law, Art. 6.

covered in one provision, as transmitting data might have an effect on the system. However, analysis shows that there is no correlation. Countries with separate provisions on data interference also include transmission in the list of prohibited acts.

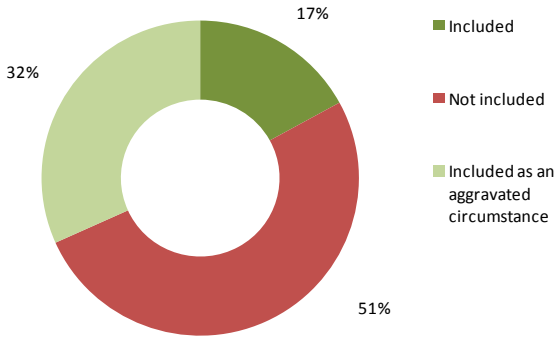
Figure 4.12: Elements constituting illegal data interference



Source: UNODC legislation review. (n=83)

Some multilateral instruments permit countries to make reservations regarding the effects caused by data interference. The Council of Europe Cybercrime Convention, for example, provides the possibility to limit criminalization of data interference to cases of serious harm.[41] The EU Decision on Attacks against Information Systems grants the freedom not to criminalize minor cases.[42]

Figure 4.13: Is harm included as a necessary element of data interference?



Source: UNODC legislation review. (n=83)

Figure 4.13 shows that at the national level, only 17 per cent of the countries examined include harm or loss as a *necessary* element of data interference. Just over 30 per cent of countries provide for *aggravating circumstances* with respect to the harm caused by data interference. Half of national laws do not refer at all to damage caused by data interference in relevant national provisions.

In the same way as computer data, computer *systems* can be damaged in various ways, such as by transmission, alteration or deletion of data, by electromagnetic interference or by cutting the system off from a power supply. System interference provisions in multilateral instruments usually include '*alteration*.' '*deletion*.' and '*transmission of data*' or any other '*manipulation*' of data or programmes. Broader definitions, however, can be found in the Commonwealth Model Law and the ITU/CARICOM/CTU Model Legislative Texts, which include not only the manipulation of data, but also cutting off the electricity supply to a computer system, causing electromagnetic interference and corrupting a computer system by any means.[43]

System interference: National example from a country in Southern Africa

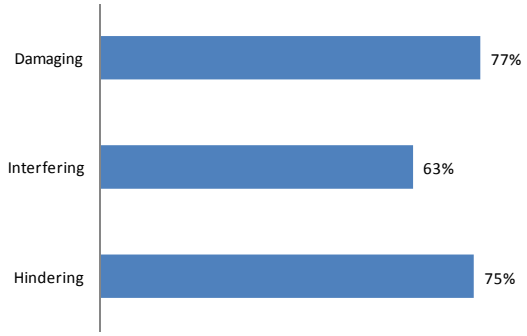
Damaging or denying access to computer system
Any person who without lawful authority or lawful excuse, does an act which causes directly or indirectly
(a) a degradation, failure, interruption or obstruction of the operation of a computer system; or
(b) a denial of access to, or impairment of any program or data stored in, the computer system,
shall commit an offence and shall, on conviction be liable to a fine not exceeding ___ and to penal servitude not exceeding ___ years.

Figure 4.14 shows that for the majority of national legislation examined, the acts of

41 Council of Europe Cybercrime Convention, Art. 4.
42 EU Decision on Attacks against Information Systems, Art. 3.
43 Commonwealth Model Law, Art. 7; ITU/CARICOM/CTU Model Legislative Texts, Art. 3(10).

'*damaging*', '*interfering*', and '*hindering*', are included. Two broad legislative trends observed are either the use of the term '*hindering by any means,*' creating a broad basis for criminalization of system interference, as well as the attachment of system interference provisions to 'illegal access' provisions, creating a narrower basis.

Figure 4.14: Acts constituting illegal system interference



Source: UNODC legislation review. (n=81)

State of mind – Many multilateral cybercrime instruments require that the crime of illegal data interference or system interference be committed '*intentionally*' or '*fraudulently.*'[44] The League of Arab States Model Law does not mention intent in its data interference provision. It does, however, require the special purpose of stopping a computer system or data functioning.[45] A different approach is taken by the Commonwealth Model Law, which explicitly requires criminalization of interference acts committed *recklessly*.[46] This creates a particularly broad basis of criminalization in light of the fact that it is often easier to interfere unintentionally with computer data or the operation of computer systems, than for objects or property in the physical world.[47] Out of 81 countries in which data interference provisions were reviewed, only six followed this approach and criminalized *reckless* or *negligent* data interference. The majority of these were not members of the Commonwealth, but were found in South America, Western Europe, and Africa.

Aggravating circumstances – Multilateral cybercrime instruments mostly do not require aggravated penalties for illegal data interference. There are two exceptions. The COMESA Draft Model Bill provides for aggravated penalties, where there is intent to cause serious harm or to threaten public safety, or intent to disrupt critical infrastructure, or for terrorist purposes.[48] The EU Directive Proposal on Attacks against Information Systems(as in the case of illegal access), requires countries to provide aggravating circumstances for the

Illegal data interference: National example from a country in South-Eastern Asia

Unauthorized modification of the contents of any computer

(1) A person shall be guilty of an offence if he does any act which he knows will cause unauthorized modification of the contents of any computer.

(2) For the purposes of this section, it is immaterial that the act in question is not directed at—

(a) any particular program or data;

(b) a program or data of any kind; or

(c) a program or data held in any particular computer.

(3) For the purposes of this section, it is immaterial whether an unauthorized modification is, or is intended to be, permanent or merely temporary.

For the purposes of this Act, a modification of the contents of any computer takes place if, by the operation of any function of the computer concerned or any other computer—

(a) any program or data held in the computer concerned is altered or erased;

(b) any program or data is introduced or added to its contents; or

(c) any event occurs which impairs the normal operation of any computer,

and any act that contributes towards causing such a modification shall be regarded as causing it.

44 Draft African Union Convention, Arts. III-19, III-20; COMESA Draft Model Bill, Art. 20-b; Council of Europe Cybercrime Convention, Art. 4; ECOWAS Draft Directive, Arts. 5, 7; EU Decision on Attacks against Information Systems, Art. 3; EU Directive Proposal on Attacks against Information Systems, Art. 4; ITU/CARICOM/CTU Model Legislative Texts, Art. 7; League of Arab States Convention, Art. 8.

45 League of Arab States Model Law, Art. 6.

46 Commonwealth Model Law, Art. 6.

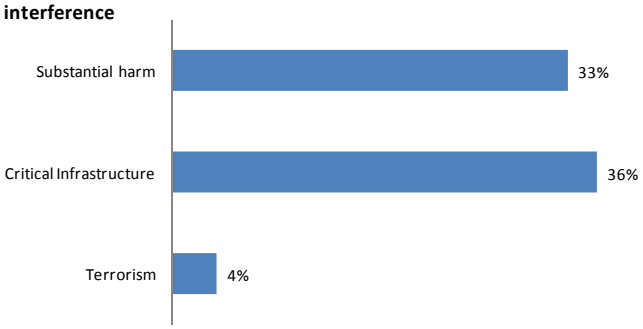
47 De Hert, P., Fuster, G. and Koops, B. J., 2006. Fighting cybercrime in the two Europes. The added value of the EU framework decision and the Council of Europe Convention. *International Review of Penal Law*, 77:6.

48 COMESA Draft Model Bill, Art. 20-c, d, e, f.

involvement of criminal organizations, through the use of tools designed to attack a significant number of information systems, or when the real identity of the perpetrator is concealed.[49]

At the national level, many countries that criminalize data interference have included aggravating circumstances that attract more severe sanctions. Figure 4.15 shows that these most often include where the interference causes *'substantial harm,'* or where it involves interference with '*critical infrastructure.*' A small number of countries in which legislation was reviewed also included aggravating circumstances where the interference is linked with terrorism. Smaller numbers of laws also included aggravating circumstances for offences committed in an organized manner, and acts committed with the intent to acquire property. A few countries have also created additional protections for particular types of data. One country in Asia, for example, has established an aggravated penalty for interference with medical and healthcare records data.

Figure 4.15: Aggravated circumstances of illegal system interference



Source: UNODC legislation review. (n=81)

Computer misuse tools

Software and other tools used to commit crimes in the digital environment, as well as victim passwords and access codes, have become an illicit commodity in underground cybercrime markets.[50] Criminalization of such 'crime objects' encounters a number of challenges, not least the fluid boundary between 'preparation' for and 'attempt' at a criminal offence, as well as the problem of 'dual-use' objects, which may be used for either innocent or criminal purposes. Nonetheless, precedents exist in the control of 'conventional' crime for the criminalization of objects such as 'burglary tools'[51] and multilateral cybercrime instruments have developed analogous offences. The Explanatory Report to the Council of Europe Cybercrime Convention, for example, notes that one rationale for the

Computer misuse tools: Commonwealth Model Law

Article 9(1) – Illegal devices

A person commits an offence if the person:

(a) intentionally or recklessly, without lawful excuse or justification, produces, sells, procures for use, imports, exports, distributes or otherwise makes available:

(i) a device, including a computer program, that is designed or adapted for the purpose of committing an offence against section 5, 6, 7 or 8; or

(ii) a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed;

with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8; or

(b) has an item mentioned in subparagraph (i) or (ii) in his or her possession with the intent that it be used by any person for the purpose of committing an offence against section 5, 6, 7 or 8.

(2) A person found guilty of an offence against this section is liable to a penalty of imprisonment for a period not exceeding ___, or a fine not exceeding ____, or both.

49 EU Directive Proposal on Attacks, Art. 10.

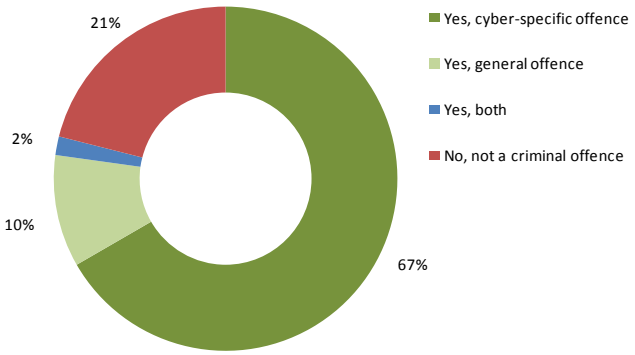
50 Europol, 2011. *Threat assessment (abridged). Internet facilitated organised crime.* iOCTA. File No.: 2530–264. The Hague. 7 January. Available at: https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf ; Fallmann, H., Wondracek, G. and Platzer, C., 2010. *Covertly probing underground economy marketplaces.* Vienna University of Technology Secure Systems Lab. Available at: http://www.iseclab.org/papers/dimva2010_underground.pdf

51 See, Fletcher, G., 1978. *Rethinking Criminal Law.* Boston: Little, Brown & Co. pp.199-202.

criminalization of computer misuse tools is in order to target acts preceding offences such as 'hacking' and to prevent the creation of black markets in such items.[52] In order to prevent overcriminalization of unknowing possession, or possession with legitimate intent, of computer misuse tools, international and regional instruments usually require a *specific* intent of use for the purposes of an offence.

Figure 4.16 shows that more than half of the countries that responded to the Study questionnaire criminalize computer misuse tools, mostly through use of a cyber-specific offence. About 20 per cent of responding countries, however, do not criminalize computer misuse tools. Analysis of primary source legislation for 70 countries that do contain such provisions reveals diverse approaches to the *object* of the crime, the *acts covered* and the *state of mind* required for the offence.

Figure 4.16: Criminalization of the production, distribution or possession of computer misuse tools

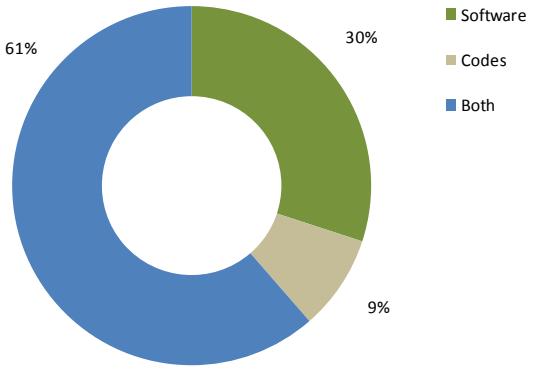


Source: Study cybercrime questionnaire. Q28. (n=57)

Offence object – Multilateral cybercrime instruments include provisions concerning two types of computer misuse tools: (i) software and devices; and (ii) passwords and codes that enable access to computer systems and data. Nine multilateral cybercrime instruments require criminalization of *both* software and codes. One instrument, however (the Commonwealth of Independent States Agreement) requires criminalization of the use and distribution of malicious software, therefore excluding hardware and codes from the object of criminalization.[53] Where used, the term 'devices' covers both hardware and software.

In addition to provisions covering tools to commit cybercrime in general, some multilateral instruments also cover devices and articles used to commit specific crimes. The EU Decision on Fraud and Counterfeiting of non-cash means of payment, for example, includes criminalization of '*instruments, articles, computer programmes and any other means peculiarly adapted for the commission of any of the offences described under Art. 2 (b)*' (counterfeiting or falsification of a payment instrument in order for it to be used fraudulently), as well as '*computer programmes, the purpose of which is the commission of any of the offences described under Art. 3*' (computer-related

Figure 4.17: Types of computer misuse tools



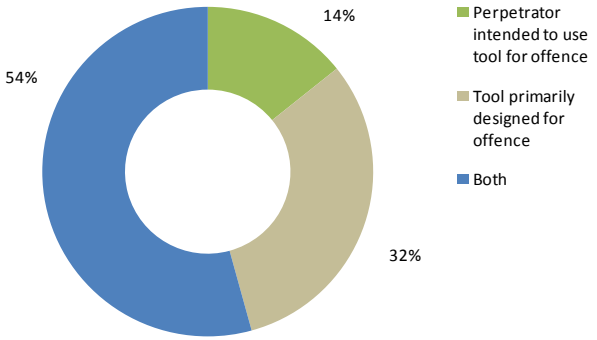
Source: UNODC legislation review. (n=70)

[52] Council of Europe, 2001. *Explanatory Report to Council of Europe Cybercrime Convention*, ETS No. 185.
[53] Commonwealth of Independent States Agreement, Art. 3(1)(b).

offences, esp. computer-related fraud).[54]

National approaches to the object of illegal device offences show some diversity. Figure 4.17 shows that the majority of countries reviewed criminalize both devices and codes. A significant number of national statutes limit criminalization, however, to either devices alone (30 per cent), or passwords and codes alone (around 10 per cent). A different approach to the object is taken in other countries, which criminalize the creation and dissemination of *computer viruses* instead of, or in addition to, software and codes. Several countries also criminalize acts related to the possession and distribution of '*articles for computer fraud*.' Provisions criminalizing this kind of device were evident in 12 of 70 countries examined.

Figure 4.18: Intent requirement for computer misuse tool offences



Source: UNODC legislation review. (n=70)

Another important characteristic of the offence is the *purpose* of the tool. Most multilateral instruments, for example, required that a 'misuse device' has been *primarily* designed for the commission of an offence. In addition, many instruments also require that the perpetrator *intends* to use the tool to commit a crime. Two multilateral instruments (the Draft African Union Convention and the Commonwealth of Independent States Agreement), however, address only the purpose of the tool and not the intent of the perpetrator. Figure 4.18 shows that, at the national level, over 50 per cent of countries reviewed also require both that the tool was primarily designed for the commission of an offence, and that the perpetrator intended to use it for such.[55] Some national approaches, however, focus only on the purpose of the tool alone, *or* the intent of the perpetrator alone.

Computer misuse tools: National example from a country in Oceania

Telecommunications and Computer Offences-

(1) No person shall: …

(f) intentionally, without right and with dishonest or otherwise unlawful intent, use, possess, produce, sell, procure for use, import, distribute or otherwise make available or attempt to use, possess, produce, sell, procure for use, import, distribute otherwise make available a device, including but not limited to a computer program, for the purpose of committing any of the offences established in paragraphs (a), (b), (c), (d) or (e);

(g) intentionally, without right and with dishonest or otherwise unlawful intent, use, possess, produce, sell, procure for use, import, distribute or otherwise make available or attempt to use, possess, produce, sell, procure for use, import, distribute or otherwise make available a computer password, access code or similar data by which the whole or any part of a telecommunications network or computer system is capable of being accessed with intent that such network or system be used for the purpose of committing nay of the offences established in paragraphs (a), (b), (c), (d) or (e); …

(2) Every person who acts in contravention of any of the provisions in subsection (1) commits an offence and is liable to the penalties provided in section ___.

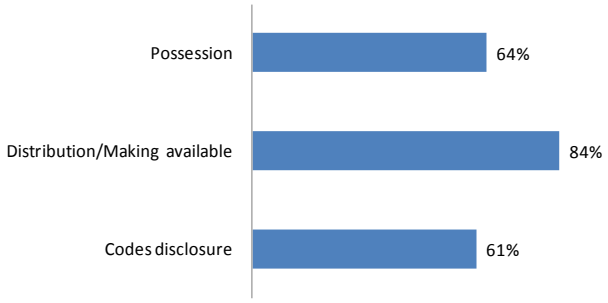
Acts covered – Multilateral instruments include a wide range of acts related to computer misuse tools, including: '*producing*', '*selling*', '*importing*', '*possessing*', '*distributing*', '*disseminating*', '*offering*', '*transferring*', and '*making available*' such tools. As illustrated in Figure 4.19, analysis of national laws

[54] EU Framework Decision 2001/413/JAI of 28 May 2001 (EU Decision on Fraud and Counterfeiting).

[55] UNODC legislation review.

shows that more than 80 per cent of countries criminalize 'dissemination'. 'Possession' of misuse tools is criminalized in close to 65 per cent of countries. Some national laws also include criminalization of acts that are not provided for by international or regional instruments but can be considered as related to computer misuse tools provisions. Many countries in the Caribbean region, for example, criminalize the act of '*unauthorized disclosure*' of passwords or access codes.

Figure 4.19: Acts concering computer misuse tools



Source: UNODC legislation review. (n=70)

Spam

It is estimated that spam accounted for around 70 per cent of global internet e-mail traffic in mid-2012.[56] Spam is an issue of consent rather than content. It is often defined as the sending of *unsolicited bulk* messages.[57] The problems caused by spam go far beyond the simple annoyance of internet users.[58] Spam consumes resources such as bandwidth, server capacity, and network infrastructure, and represents an entry point for the spread of malware and phishing of access codes and financial information. It is thus linked with conduct such as data and system interference – directly and indirectly endangering the integrity and availability of computer data and systems.

Spam: COMESA Draft Model Bill

Article 19 – Unauthorized Access to Computer Programs, Computer Data, Content Data, Traffic Data

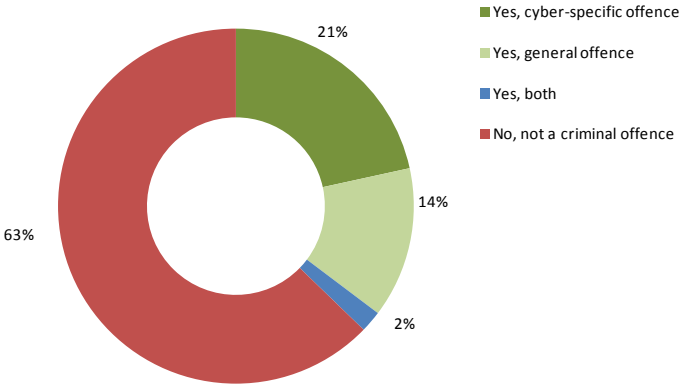
...

(g) Spamming

A person who transmits any unsolicited electronic information to another person for purposes of illegal trade or commerce or other illegal activity, shall have committed a criminal offense punishable by a fine of [amount]_____ and/or imprisonment for a period of _____ years, or to both.

Nonetheless, harmonization of legal approaches towards spam is far from complete.[59] Two multilateral (non-binding) cybercrime instruments propose the criminalization of spam – the COMESA Draft Model Bill (Art. 19), and the ITU/CARICOM/CTU Model Legislative Texts (Art. 15). None of the binding multilateral cybercrime instruments include criminal provisions on spam, although the preamble to the EU

Figure 4.20: Criminalization of the sending or controlling of the sending of SPAM



Source: Study cybercrime questionnaire. Q33. (n=51)

56 Symantec Intelligence Report, June 2012; Kaspersky Lab Report, June 2012.

57 For a working (rather than legal) definition, see http://www.spamhaus.org/consumer/definition/

58 Sorkin, D., 2001. Technical and Legal Approaches to Unsolicited Electronic Mail. *University of San Francisco Law Review*, 35(2):325-384

59 De Hert, P., Fuster, G., Koops, B. J., 2006. Fighting cybercrime in the two Europes. The added value of the EU framework decision and the Council of Europe Convention. *International Review of Penal Law*, 77(3-4):503-524.

Directive on Data Protection provides that '*it is necessary to prohibit the use of false identities or false return addresses or numbers while sending unsolicited messages for direct marketing purposes.*'[60] In addition, Article 13(3) of the same Directive requires States to '*take appropriate measures*' to ensure that, '*free of charge, unsolicited communications for purposes of direct marketing*' are not allowed without consent. The Directive does not, however, explicitly require the establishment of a particular offence under the domestic laws of Member states.

Responses to the Study cybercrime questionnaire indicate that sending or controlling sending of spam is a criminal offence only in around one third of responding countries. Both cyber-specific and general offences are used. Review of available primary source national legislation resulted in the identification of only nine countries out of almost 100 in which specific criminal provisions on spam could be identified. The *object* of *spam* offences varies from '*unsolicited bulk messages*' to criminalization of falsification of '*message headers*' or '*origin*'. One country in the Americas, for example, has adopted criminal provisions punishing the falsification of e-mail subject lines. In some countries, it was also possible to identify administrative sanctions for sending or controlling sending of spam.

Spam: National example from a country in Southern Asia

Penalty for damage to computer, computer system, etc.

If any person…

(h) for the purpose of advertisement of goods and services, generates or causes generation of spams or sends unwanted electronic mails without any permission of the originator or subscriber;…
(2) Every person who acts in contravention of any of the provisions in subsection (1) commits an offence and is liable to the penalties provided in section ___.

The main *acts* that are the subject of spam criminalization include the '*transmission*' of unsolicited, multiple e-mails or acts that mislead the recipient of the message – such as by '*manipulation*' of the header or originating information. As regards the mental element, the COMESA Draft Model Bill requires that the act be *intentional* and committed for illegal purposes. The ITU/CARICOM/CTU Model Legislative Texts also require the criminalization of intentional acts. Intentionality is also required by those national provisions that could be identified and analysed.

While the problem of spam is not explicitly tackled by any binding international instrument, a number of elements of the threat posed by spam, such as malware and phishing, are covered through international and regional provisions protecting the integrity, availability and confidentiality of computer data and systems.

Computer-related fraud and forgery

The protected legal interest in crimes against the confidentiality, integrity and availability of computer data and systems is the integrity of computer information and data itself. In contrast, criminal provisions on computer-related fraud and forgery protect interests in property, financial assets and the authenticity of documents.[61] At the international and regional level, eight instruments contain provisions on criminalization of computer-related fraud.[62] Acts covered in the instruments

60 EU Directive on Data Protection, Preamble (43).

61 Sieber, U., 1998. *Legal Aspects of Computer-Related Crime in the Information Society COMCRIME-Study.* Available at: www.edc.uoc.gr/~panas/PATRA/sieber.pdf.

62 Draft African Union Convention, Art. III-26, III-41; COMESA Draft Model Bill, Art. 24; Council of Europe Cybercrime Convention, Art. 8; ECOWAS Draft Directive, Art. 10; EU Decision on Fraud and Counterfeiting, Art. 2; ITU/CARICOM/CTU Model Legislative Texts, Art. 12; League of Arab States Convention, Arts. 10, 11; League of Arab States Model Law, Arts. 10-12).

concern the manipulation of computer data, or interference with a computer system, that leads to economic benefit for the offender or another person.

Six instruments also contain specific provisions on forgery.[63] Acts covered by computer-related forgery provisions include the alteration, deletion, transmission and other manipulation of computer data, resulting in inauthentic date that is intended to be acted upon or used as if it were authentic.

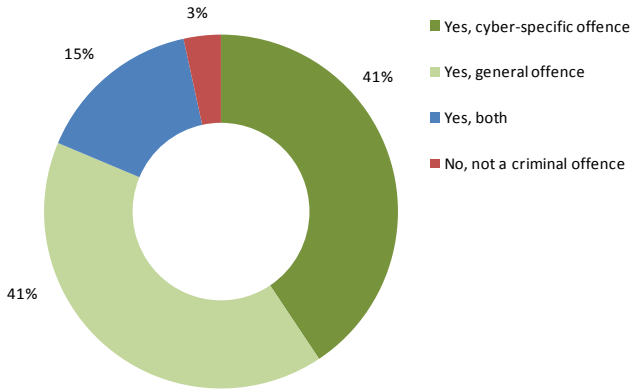
Computer-related fraud: Council of Europe Cybercrime Convention

Article 8

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
a any input, alteration, deletion or suppression of computer data;
b any interference with the functioning of a computer system,
with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

At the national level, however, the situation varies significantly concerning the existence of cyber-specific provisions for fraud and forgery. Responding countries to the Study questionnaire indicated that computer-related fraud or forgery was covered by existing general legislation (over 40 per cent). Almost the same proportion reported the existence of a cyber-specific offence, while 15 per cent of countries use both approaches.[64]

Figure 4.21: Criminalization of computer-related fraud or forgery



Source: Study cybercrime questionnaire. Q30. (n=59)

This diversity derives in part from differences between national legal systems in the extent to which 'traditional' offences can be applied in a 'cyber' environment. Traditional fraud offences for example often require the direct deception of a '*person*' and may suffer challenges in their extension to acts committed through the manipulation of a computer system or computer data.[65] Similarly, traditional forgery offences often require alteration of a '*visual representation*', a requirement which may not, depending upon the national legal approach, be satisfied by alteration of intangible data on electronic devices.[66]

Computer-related forgery: Draft African Union Convention

Article III – 8

Each Member State of the African Union shall take the legislative measures to set up as a penal offense the fact of producing or manufacturing a range of digital data by fraudulently introducing, deleting or suppressing computerized data held, processed or transmitted by a computer system, resulting in fake data, with the intention that the said data would be taken into account or used for illegal purposes as if they were the original data

63 Draft African Union Convention, Art. III-24; Council of Europe Cybercrime Convention, Art. 7; COMESA Draft Model Bill, Art. 23; ITU/CARICOM/CTU Model Legislative Texts, Art. 11; League of Arab States Model Law, Art. 4; ECOWAS Draft Directive, Art. 8.

64 Study cybercrime Questionnaire. Q30.

65 Sieber, U., 2008. Mastering complexity in the global cyberspace : The harmonization of computer-related criminal law. In : Delmas-Marty, M., Pieth, M. and Sieber, U., (eds.) *Les chemins de l'Harmonisation Penale/Harmonising Criminal Law. Collection de L'UMR de Droit Compare de Paris*. Vol. 15. Paris: Société de législation comparé.

66 *Ibid.*

In order to address such legal challenges, national cyber-specific provisions for fraud often focus on the manipulation of computer data or systems with dishonest or fraudulent intent, rather than on the element of deception of an individual. In some countries, computer-related fraud provisions also criminalize the *unauthorized* use of data, in addition to the use of *false* data (see example box from a country in Southern Asia). This can lead to broad application of computer-related fraud provisions, for example, to all cases of computer use for illicit enrichment.[67] A number of countries continue to amend national laws in order to introduce cyber-specific offences for computer-related fraud. One country in Eastern Europe, for example, has recently adopted a new article on computer-related fraud in its criminal code after more than a decade of prosecuting cases of computer fraud under a combination of general fraud and illegal access provisions. Although it had previously supported this approach, the reform was initiated by the Supreme Court with a view to ensuring more efficient prosecution of suspects and removing any remaining legal uncertainty about the applicability of traditional fraud provisions.

Combining computer-related fraud and forgery: National example from a country in Southern Africa

(1) A person who performs any of the acts described under this Part, for the purposes of obtaining any unlawful advantage by causing forged data to be produced, with the intent that it be considered or acted upon as if it were authentic, commits an offence and shall on conviction be liable to a fine ___ or to imprisonment ____, or to both.
(2) A person who, with intent to procure any advantage for himself or herself or another person, fraudulently causes loss of property to another person by-
(a) any input, alteration, deletion or suppression of data; or
(b) any interference with the functioning of a computer or computer system,
commits an offence and shall on conviction be liable to a fine ____ or to imprisonment_____, or to both.

Some countries also apply provisions on theft to cases of computer fraud by, considering computer data to be fall under definitions of '*goods*' or '*things*.' This approach is taken by some countries in Western Europe, Northern Europe, and North America. Several countries further have provisions on '*qualified theft*' or larceny which include the use of computer systems for commission of the offence (see example box from a county in Western Asia).

National provisions on computer-related *forgery* typically require two necessary elements: (i) the *alteration* or *manipulation* of computer data, and (ii) a specific intent to use the data as if they were authentic. Alternatively, countries may extend the definition of the object of traditional forgery. A number of countries in Europe, for example, have covered computer-related forgery by extending the definition of '*document*' to include computer data. Other countries apply general provisions to computer-related forgery without amending legislation if traditional provisions of forgery can be interpreted to include digital documents, signatures and data.

Computer-related forgery: National example from a country in Southern Europe

Article --- Computer Forgery
(1) Whoever, without authorization, develops, installs, alters, deletes or makes unusable computer data or programs that are of significance for legal relations in order for them to be used as authentic, or whoever uses such data or programs shall be punished by a fine of by imprisonment not exceeding _____.
(2) If the criminal offence referred to in paragraph 1 of this Article is committed in connection with the computer data or programs of a governmental body, a public institution or a company of special public interest, or if significant damage is caused, the perpetrator shall be punished by imprisonment for _____.

[67] See Sieber, U., 1985. *Informationstechnologie und Strafrechtsreform*. Cologne: Carl Heymanns Verlag, p.39.

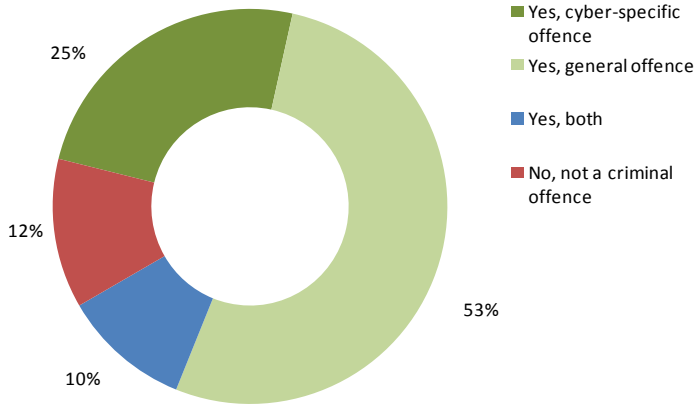
Identity-related offences

Global connectivity, the automation of data processing, and the development of non-face-to-face transactions have generated increased opportunities for theft of identity-related information and personal data through computer systems.[68] Such crime targets both 'traditional' identifying information, as well as new types of identification information, including credit card numbers, bank account information, passport and driving license numbers, internet accounts, passwords and IP addresses. This information can be the subject of several constitutive acts of identity theft, including the obtaining, transferring, and use of identity-related information. Data can be obtained, for example, via illegal access to computer systems, including through use of malware, by the use of phishing (itself often constituting computer-related forgery), or by illegal acquisition of computer data, such as by corporate 'insiders.'

Identity-related offences: ITU/CARICOM/CTU Model Legislative Texts

Article 14
A person who, intentionally without lawful excuse or justification or in excess of a lawful excuse or justification by using a computer system in any stage of the offence, intentionally transfers, possesses, or uses, without lawful excuse or justification, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a crime, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding[amount], or both.

Figure 4.22: Criminalization of computer-related identity offences



Source: Study cybercrime questionnaire. Q31. (n=57)

A range of approaches exist regarding criminal law responses to the acts of obtaining, transferring and using identification data for criminal purposes. At the international and regional level, provisions concerning identity theft can be found in only one (non-binding) instrument – the ITU/CARICOM/CTU Model Legislative Texts (Art. 14). This provision covers acts committed with the use of a computer at any stage of the offence involving intentional transfer, possession or use, without lawful excuse or justification, of '*a means of identification of another person*' with the '*intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a crime.*'

Identity-related offence: National example from a country in the Caribbean

Identity theft. Article ---

A person who uses a computer or knowingly causes a computer to perform any function for the purpose of securing access to any program or data held in that computer or in any other computer with intent to impersonate another person or steal or impersonate their identity commits an offence and is liable on conviction to a fine of ____ and to imprisonment for _____.

At the national level, country responses to the Study questionnaire show that a comparatively small proportion of countries – 25 per cent – report the existence of a cyber-specific provision for identity-related offences. In contrast, more

[68] UNODC, 2011. *Handbook on Identity-related Crime.* Available at: http://www.unodc.org/documents/treaties/UNCAC/Publications/Handbook_on_ID_Crime/10-57802_ebooke.pdf

than 50 per cent of countries reported the use of general provisions. Around 10 per cent of countries reported that identity-related acts do not constitute a criminal offence.

Analysis of primary source legislation shows that, for cyber-specific identity-related offences, the *object* of identity theft is usually defined as '*data*' (or '*personal data*') or '*identification information*.' Where provisions exist, they do not always cover all acts that can constitute the possible components of identity theft. Some countries do not, for example, include the 'transfer' of personal data, but rather limit criminalization to acts such as 'using' and 'obtaining' the means of identification. Others cover only 'obtaining', or do not include obtaining or use at all (see example box from a country in the Caribbean). Some national laws go further and also criminalize creating false personal data. Overall, a review of primary source legislation suggests that the number of countries with cyber-specific identity offences is relatively low, and for those that do, significant divergence in approaches exists. Where identity-related offences are covered by general laws, this can be through a number of different provisions, including on illegal access, illegal data interference, computer misuse tools, computer-related forgery and computer-related fraud.

Child pornography offences

Almost all images containing child pornography are transmitted electronically, through bilateral and multilateral exchanges.[69] Interests protected by the criminalization of child pornography include the protection of minors from abuse, and the disruption of markets in child pornographic images, that may encourage offenders to seek to produce and supply further images.[70] At the international and regional levels, nine identified instruments include provisions criminalizing acts related to child pornography.[71] Although international frameworks demonstrate many similarities with respect to the criminalization of child pornography, differences also relate to the object, age of children, and acts covered.

Child pornography: Optional Protocol to the Convention on the Rights of the Child

Article 3

1. Each State Party shall ensure that, as a minimum, the following acts and activities are fully covered under its criminal or penal law, whether such offences are committed domestically or transnationally or on an individual or organized basis: …
(c) Producing, distributing, disseminating, importing, exporting, offering, selling or possessing for the above purposes child pornography as defined in article 2. …
3. Each State Party shall make such offences punishable by appropriate penalties that take into account their grave nature.

At the national level, over 80 per cent of countries responding to the Study questionnaire indicated that child pornography is a criminal offence. The majority of countries reported that such acts are criminalized by way of a general offence. As acts involving child pornography may be perpetrated through a wide range of media – including 'offline' images – a general 'technology and media neutral' approach is preferred to a computer-specific approach by many countries. A number of country responses to the Study questionnaire suggested that child pornography was criminalized within the context of pornography generally. This was confirmed by analysis of source legislation, during which two countries with general provisions on pornography, including child pornography, were identified. For countries which do not have specific provisions on child pornography, it is possible that such material can be prosecuted using broader laws on obscenity or offensive material.

69 UNODC, 2010. *The Globalisation of Crime. A Transnational Organized Crime Threat Assessment. Chapter 10.* Available at: http://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf, p.212.

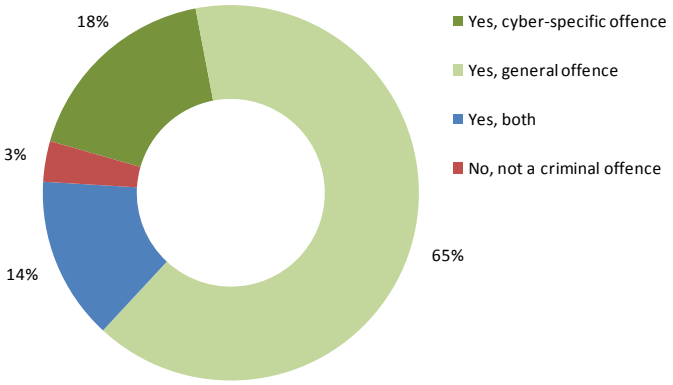
70 See Hamilton, M., 2011-2012. The child pornography crusade and its net-widening effect. *Cardozo Law Rev,* 33(4):1679-1732.

71 Draft African Union Convention, Art. III-29 to III-32; Commonwealth Model Law, Art. 10; Council of Europe Cybercrime Convention, Art. 9; Council of Europe Child Protection Convention, Art. 20; ECOWAS Draft Directive, Arts. 14-17; EU Directive on Child Exploitation, Art. 5; ITU/CARICOM/CTU Model Legislative Texts, Art. 13; League of Arab States Convention, Art. 12; United Nations OP-CRC-SC, Art. 3.

Analysis of legislation from those countries with specific child pornography provisions shows many similarities as well as some differences between the *offence object* and the *acts covered*.

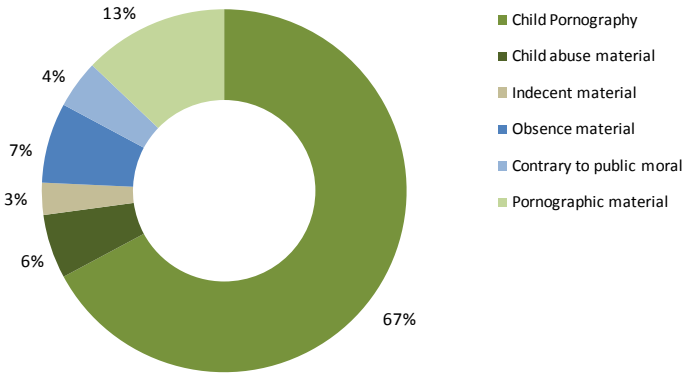
Offence object – Most international and regional instruments use the term '*child pornography*' to define the object of the offence. The League of Arab States Convention uses the term '*pornographic material depicting a child*'. Figure 4.24 shows that terminology varies at the national level. For 70 countries whose provisions were reviewed, almost 70 per cent use the term '*child pornography.*' Just over 10 per cent use the term '*pornographic material depicting a child.*' Other variants include '*obscene material depicting a child,*' '*child abuse material,*' '*material contrary to public morals involving a child,*' and '*indecent material depicting a child.*' Whether differences in terms translate into practical differences in the nature of material criminalized cannot be assessed from legislative texts alone, as provisions are also subject to interpretation by national judicial authorities.

Figure 4.23: Criminalization of computer-related production, distribution or possession of child pornography



Source: Study cybercrime questionnaire. Q36. (n=57)

Figure 4.24: Terminologies used in computer-related child pornography provisions



Source: UNODC legislation review. (n=70)

Legislation can, however, define the scope of media included within the offence. Some international and regional instruments, for example, refer to '*visual material*' and '*texts*' that depict child pornography. Defining included media in this way may risk, however, excluding audio material. A number of instruments (including the ITU/CARICOM/CTU Model Legislative Texts and the EU Directive on Child Exploitation) therefore refer to '*any representation, by whatever means.*' The Council of Europe Cybercrime Convention and the Commonwealth Model Law, on the other hand, refer to material which '*visually depicts*' child pornography, thereby excluding audio material. At the national level, source legislation review shows that around one-third of countries examined limit the object of criminalization to visual material or visual representation. The remaining countries include text, audio

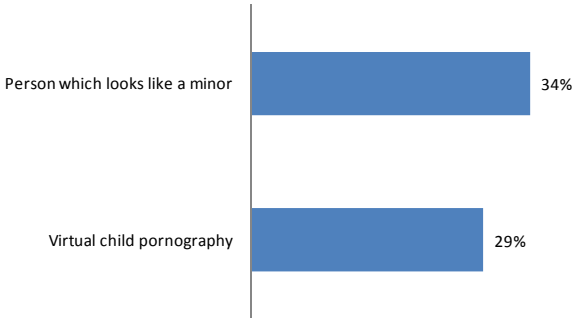
Child pornography: National example from a country in Western Europe

A term of imprisonment of not more than __ years or a fine of ___ shall be imposed on any person who disseminates, offers, publicly displays, manufactures, imports, forwards, exports, acquires, or possesses an image – or a data carrier containing an image – of a sexual act in which a person who has apparently not yet attained the age of eighteen is involved or appears to be involved, or who gains access to such an image by means of a computerized device or system or through a communication service.

files (less frequently), or refer to any representation whatsoever.[72]

A second difference between legal approaches concerns material that does not involve children in production. This includes computer-simulated representations or realistic images of a non-existent child, or material involving persons who have reached the age of majority (for the purposes of the child pornography prohibition) but who look like minors. The majority of international or regional instruments include this type of material within the scope of criminalization,[73] although some instruments permit countries not to criminalize realistic images.[74] At the national level, not all countries follow this approach. For the countries from which legislation was reviewed, 34 per cent cover realistic pictures of adults who '*look like minors*,' or which '*seemingly involve minors*,' or which are '*realistic images of minors*.' Only 29 per cent of countries examined provide for criminalization of '*fictitious*' or '*virtual*' child pornography.

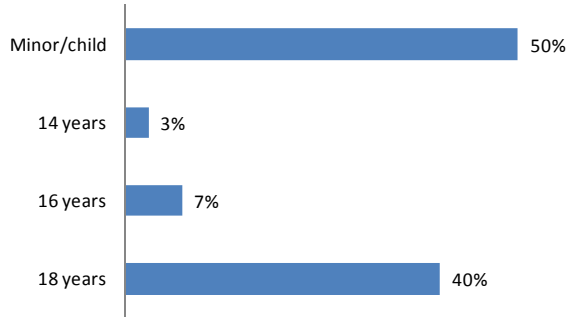
Figure 4.25: Criminalization of the computer-related production, distribution or possession of simulated child pornography materials



Source: UNODC legislation review. (n=70)

A third difference is the age of the child involved in the pornographic representation. Article 1 of the United Nations Convention on the Rights of the Child defines a child as every human being below the age of eighteen years. It includes the proviso however: '*unless*' under the law applicable to the child '*majority is attained earlier*.'[75] While States Parties are therefore free, in principle, to apply age limits lower than 18 in definitions of child pornography, the United Nations Committee on the Rights of the Child has, on a number of occasions, recommended that definitions should cover *all* children under the age of 18 years.[76] Other instruments refer to different age limits. The Council of Europe Cybercrime Convention, for example, specifies that the term '*minor*' shall include all persons under 18 years of age, but allows that a State party may set a lower age-limit, which '*shall not be less than 16 years*.' Other instruments, such as the League of Arab States Convention or the Commonwealth

Figure 4.26: Specifications concerning the age of the victim in computer-related child pornography provisions



Source: UNODC legislation review. (n=70)

[72] UNODC legislation review.

[73] Covered explicitly in: Draft African Union Convention, Art. III-1; Commonwealth Model Law, Art. 10; Council of Europe Cybercrime Convention, Art. 9; Council of Europe Child Protection Convention, Art. 20; ECOWAS Draft Directive, Art. 1; EU Directive on Child Exploitation, Art. 2(c); ITU/CARICOM/CTU Model Legislative Texts, Art. 3(4); United Nations OP-CRC-SC, Art. 2(c).

[74] Council of Europe Cybercrime Convention; EU Directive on Child Exploitation – when material was used for the purpose of its production and there is no risk of dissemination.

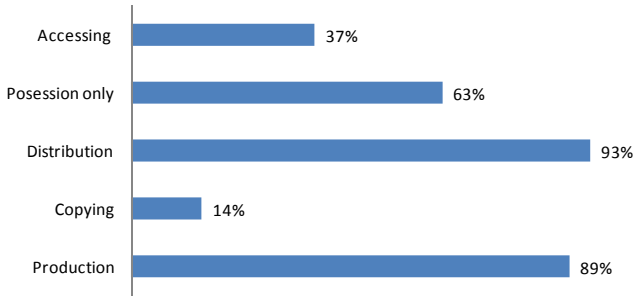
[75] United Nations Convention on the Rights of the Child, Art.1.

[76] See, for example, CRC/C/OPSC/MNE/CO/1 (2010); CRC/C/OPSA/NOR/CO/1 (2005); CRC/C/OPSC/YEM/CO/1 (2009); and CRC/C/CUB/CO/2/ (2011).

Model Law, use the term '*child*' or '*minor*' without setting an age limit.

At the national level, identifying the age to which child pornography provisions apply is not straightforward. Many countries refer to the term '*minor*' or '*child*' without specifying an age in the article itself. Rather, relevant ages may be found in other parts of national legislation – including child protection or child rights legislation. Figure 4.26 shows that for many of the available criminal law provisions analysed, it was not possible to easily identify the relevant age (without detailed analysis of other parts of the national law). Where it was possible to identify the age from national criminal law, the large majority of provisions referred to the age of 18 years. Criminal laws in only a few countries contained an age of 16 or 14 years for the purposes of defining child pornography. In this respect, the United Nations Committee on the Rights of the Child has expressed particular concern over the use of age limits of 14 years.[77]

Figure 4.27: Acts constituting child pornography offences



Source: UNODC legislation review. (n=70)

Acts covered – The majority of international and regional instruments require criminalization of a wide range of actions associated with child pornography, including '*production*', '*offering*', '*making available*', '*distribution*', '*transmission*', and '*possession*'. Some instruments also criminalize knowingly '*obtaining access*' to child pornography.[78] National laws show some diversity with respect to which of these acts are included. As can be seen in figure 4.27, '*production*' and '*distribution*' of child pornography are most commonly criminalized – by around 90 per cent of national legislative provisions reviewed. Over 60 per cent of countries reviewed criminalize '*possession,*' with almost 40 per cent including provisions on '*accessing*' child pornography. In some countries, the extent to which 'possession' provisions can be applied in the case of online viewing of still or moving images remains unclear. A number of countries in Europe include online viewing of child pornography within the scope of possession due to the fact that viewing pictures necessarily includes the copying of images into computer memory and/or temporary internet cache files. Other countries have created solutions such as a requirement for '*habitual activities*' on the part of the perpetrator.

Computer-related solicitation or 'grooming' of children

Criminal laws on online child 'grooming' represent a form of criminalization of acts preparatory to 'offline' abuse of children.[79] Two multilateral instruments, both from the European region – the Council of Europe Child Protection Convention (Art. 23) and the EU Directive on Child Exploitation (Art. 6) – require criminalization of such acts. The core elements of the offence include the '*intentional proposal, through information and communication technologies,*' by an adult to '*meet*' a

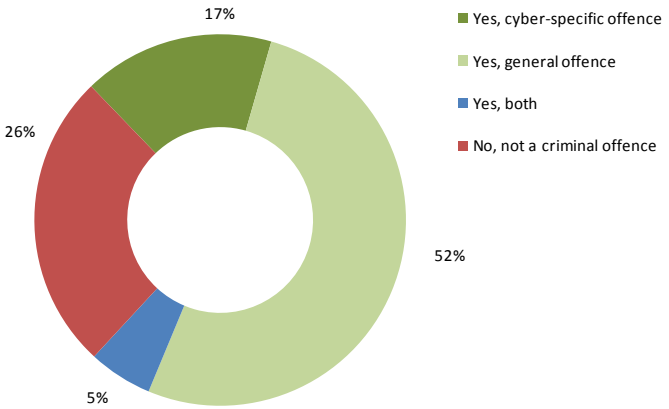
77 See, for example, CRC/C/OPSC/EST/CO/1 (2010) and CRC/C/OPSC/AUT/CO/1 (2008). The Committee also considers that the use of offence conditions such as 'intent to disseminate' and 'where the minor does not consent' for child pornography offences involving children between 14 and 18 years are incompatible with the Optional Protocol to the Convention on the Rights of the Child.

78 Draft African Union Convention; Council of Europe Child Protection Convention; EU Directive on Child Exploitation; ITU/CARICOM/CTU Model Legislative Texts.

79 Eneman, M., Gillespie, A. A., Bernd, C. S., 2010. Technology and Sexual Abuse: a Critical Review of and Internet Grooming Case. *ICIS 2010 Proceedings. Paper 144*; Kool, R., 2011. Prevention by All Means? A Legal Comparison of the Criminalization of Online Grooming and its Enforcement. *Utrecht Law Review*, 7(3):46-69.

child '*for the purpose*' of committing an offence. In order for the offence to be committed, both instruments also require '*material acts*' leading to such a meeting, by the perpetrator.

Figure 4.28: Criminalization of computer-related solicitation or 'grooming' of children



Source: Study cybercrime questionnaire. Q37. (n=54)

At the national level, country responses to the Study questionnaire show divergent approaches. Almost 70 per cent of countries report that grooming is an offence, although the majority of these countries report use of a general offence, rather than a cyber-specific offence. In over 25 per cent of countries, the act does not constitute a criminal offence.

Analysis of available primary source legislation led to the identification of specific provisions covering online solicitation of children in 17 out of 97 countries. About half of these countries are located in Europe. This likely reflects the influence of the grooming provisions in the Council of Europe Child Protection Convention and the EU Directive on Child Exploitation. Criminalization of grooming was also, however, identified in some national laws of countries in Asia, Africa, Americas and Oceania.

Grooming: National example from a country in Southern Europe

Whoever uses the Internet, telephone or any other information and communication technology to contact a person under the age of thirteen years and proposes to meet that person in order to commit any of the offences described in Articles ____, as long as such a solicitation is accompanied by material acts aimed at such an approach, shall be punished with the penalty of ____ years imprisonment or a fine of ____, without prejudice to the relevant penalties for the offences actually committed. The penalties shall be imposed in the upper half when the approach is obtained by coercion, intimidation or deceit.

Grooming: Council of Europe Child Protection Convention

Article 23 – Solicitation of children for sexual purposes

Each Party shall take the necessary legislative or other measures to criminalize the intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age set in application of Article 18, paragraph 2, for the purpose of committing any of the offences established in accordance with Article 18, paragraph 1.a, or Article 20, paragraph 1.a, against him or her, where this proposal has been followed by material acts leading to such a meeting.

Computer-related copyright and trademark offences

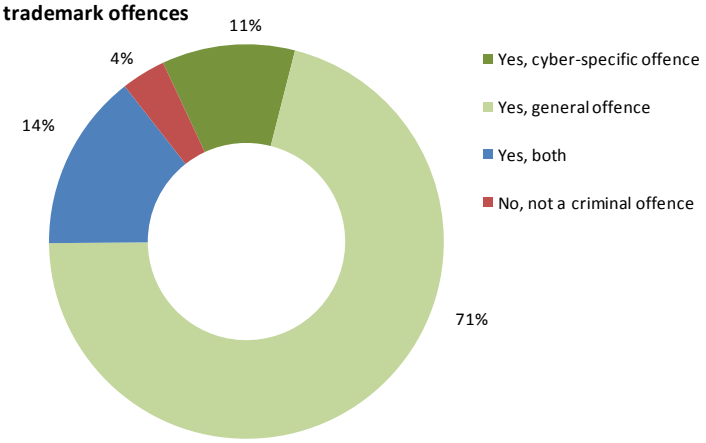
The international framework in the field of intellectual property law is somewhat wider than the 'cybercrime' international and regional instruments considered directly by this Study. Key actors and instruments include the World Trade Organization and the TRIPS Agreement,[80] (which, for the first time, included criminal provisions at the international level for commercial copyright violations), as well as the World Intellectual Property Organization (WIPO) Copyright Treaty[81] and

[80] *Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)*, adopted on 15 April 1994.
[81] *World Intellectual Property Organization Copyright Treaty,* signed on 20 December 1996.

Performances and Phonograms Treaty.[82] More recently, the Anti-Counterfeiting Trade Agreement (ACTA) aimed to consolidate criminal provisions on wilful trademark counterfeiting or copyright or related piracy rights on a commercial scale.[83] The European Parliament voted against the Agreement in 2012. At the European Union level, a number of pieces of legislation deal with aspects of copyright and related rights, but none of them explicitly include criminal provisions.[84] In 2005, the European Parliament drafted a proposal for a framework decision and a directive on measures concerning criminal copyright law committed on a commercial scale.[85] This directive was revised in 2006 but has not yet been adopted.[86]

At the national level, developments in the last decade have been characterized by an increase in sanctions for copyright offences, in particular for cases of commercial and organized acts. The Council of Europe Cybercrime Convention, for example, provides for criminalization of infringement of copyright and related acts where '*committed wilfully, on a commercial scale and by means of a computer system*.'[87] At the national level, responding countries to the Study cybercrime questionnaire indicated a high level of criminalization of copyright and trademark offences, with over 80 per cent of countries stating that such acts could be a crime. The vast majority of these countries reported use of general offences rather than cyber-specific offences.

Figure 4.29: Criminalization of computer-related copyright and trademark offences



Source: Study cybercrime questionnaire. Q32. (n=55)

In practice, the large amount of infringing material on the internet (see Chapter Two (The global picture)) often means that law enforcement resources are not sufficient to prosecute the mass of possible cases. For this reason, many states also support new concepts involving c*ivil law* measures, such as written warnings, damage claims and the right to information. In addition, some countries have developed 'two strikes' and 'three strikes' models. These concepts oblige internet service providers to register IP addresses of copyright infringers, to send warning notices to first-time offenders, and to take responsibility for sanctioning of repeat offenders, or to collaborate by notifying right-holders or authorities.[88]

Discussion

The above analysis shows both similarities and divergences in national criminalization

82 *WIPO Performances and Phonograms Treaty*, signed on 20 December 1996.
83 See Arts. 23 et seq. of the *Anti-Counterfeiting Trade Agreement (ACTA)*.
84 Sieber, U., Brüner, F.H., Satzger, H., Von Heintschel-Heinegg, B. (eds.) 2011. *Europäisches Strafrecht*, pp.442 et seq.
85 Proposal for a directive on criminal measures aimed at ensuring the enforcement of intellectual property rights and proposal for a framework decision to strengthen the criminal law framework to combat intellectual property offences from 12 August 2005, COM (2005)276 final.
86 Amended proposal for a directive on criminal measures aimed at ensuring the enforcement of intellectual property rights from 26.4.2006, COM (2006) 168 final.
87 Council of Europe Cybercrime Convention, Art.10.
88 See Bridy, A., 2010. Graduated Response and the Turn to Private Ordering in Online Copyright Enforcement. *Oregon Law Review*, 89:81-132; Stamatoudi, I., 2010. *Copyright Enforcement and the Internet*. Alphen aan den Rijn, Netherlands: Kluwer Law International; Haber, E., 2011. The French Revolution 2.0: Copyright and the Three Strikes Policy. *Harvard Journal of Sports & Entertainment Law,* 2(2):297-339.

approaches to cybercrime. It is clear that, in some cases, divergences found at the national level are also present at the international level. Examples of these include the inclusion, or not, of 'illegal remaining' in multilateral instruments; the limitation, or not, of interception to 'non-public' transmissions; the possibility for criminalization of 'reckless' data or system interference; and the inclusion, or exclusion, of 'access codes' in computer misuse tool provisions. As discussed in Chapter Three (Legislation and frameworks), it is challenging to trace the exact influence of binding and non-binding instruments on national legislation. It is possible, in some cases, that a two-way process is at work – with national legislative approaches influencing the development of international and regional instruments, and *vice versa*. While such analysis can be perceived as merely technical, the details of cybercrime criminal offences matter. As discussed in Chapter Seven (International cooperation), for example, in some countries detailed offence aspects such as the 'use of technical means' to commit an offence (in the case of illegal interception, for instance) can be considered to be *constituent elements* of the crime – meaning that there is no crime unless they are present. In such circumstances, the details of the crime can have an impact on requirements for dual criminality and, ultimately, on effective international cooperation.

On the other hand, the detailed analysis reveals a number of good practices in the development of criminal laws for cybercrime acts. The creation of a clear distinction in national laws between illegal *access* to, and *interference* with, computer systems and data, for example, is important in order to ensure that separate acts can be correctly distinguished. The use of aggravating circumstances may be an effective mechanism for tailoring 'core' offences to particular national concerns, while maintaining basic offences that can be harmonized with international and regional standards. In order to avoid over-criminalization, many countries ensure that provisions on computer-misuse tools require both that the tool is primarily designed for the commission of an offence, and that the perpetrator intended to use it for such. Requirements of intentionality with respect to illegal interference with computer data and systems are also important for ensuring that negligent or reckless acts are not subject to disproportionate criminal sanctions.

The balance of appropriate criminalization is even more challenging with respect to computer content-related offences than it is for offences against the confidentiality, integrity and accessibility of computer systems. Even in an area well covered by international standards such as child pornography, for example, state approaches show divergence with respect to the inclusion, or exclusion, of simulated material, and regarding the age of the child protected. One key external standard that offers guidance in this area is international human rights law. The next section of this Chapter examines the contribution that this body of international law can make in assisting states to achieve an acceptable balance between crime prevention and control, and the protection of individual liberties.

4.3 International human rights law and criminalization

KEY RESULTS:

- The increasing use of social media and user-generated internet content has resulted in regulatory responses from government, including the use of criminal law, and calls for respect for rights to freedom of expression
- Countries report varying boundaries to expression, including with respect to defamation, contempt, threats, incitement to hatred, insult to religious feelings, obscene material, and undermining the state
- The socio-cultural element of some limitations is reflected not only in national law, but also in multilateral instruments. Some regional cybercrime instruments, for example, contain broad offences regarding the violation of public morals, pornographic material, and religious or family principles or values
- International human rights law acts both as a sword and a shield, requiring criminalization of (limited) extreme forms of expression, while protecting other forms. Some prohibitions on freedom of expression, including incitement to genocide, hatred constituting incitement to discrimination, hostility or violence, incitement to terrorism, and propaganda for war, are therefore required for states that are party to relevant international human rights instruments
- For other forms of expression, the 'margin of appreciation' allows leeway to countries in determining the boundaries of acceptable expression in line with their own cultures and legal traditions
- Nonetheless, international human rights law will intervene at a certain point. Penal laws on defamation, disrespect for authority, and insult, for example, that apply to online content will face a high threshold of demonstrating that the measures are proportionate, appropriate, and the least intrusive possible
- Where content is illegal in one country, but legal to produce and disseminate in another, States will need to focus criminal justice responses on persons accessing content within the national jurisdiction, rather than on content produced outside of the country

International human rights law both prescribes and prohibits criminalization in the area of cybercrime. Jurisprudence around the area of freedom of speech is particularly developed in assisting countries to place boundaries around criminalization of expression in areas as diverse as hate speech, incitement to terrorism, defamation, obscenity and insult.

Human rights as a 'shield' and 'sword'

Over 30 years ago, the Chair of the then United Nations Committee on Crime Prevention and Control[89] stated that '*Crime is what is defined by law as such. On the other hand, the definition must take into account the existence of, and respect for human rights and not merely be the expression of arbitrary power.*'[90] In other words, national criminal laws are not to be excluded from the oversight of international human rights law.[91]

---

89 The Committee was established by resolution of the United Nations Economic and Social Council in May 1971. See United Nations Economic and Social Council. Resolution 1548(L), 1971.

90 López-Rey, M., 1978. Crime and Human Rights. *Federal Probation* 43(1):10-15, p.11.

91 For the purposes of this Study, the human rights contained in customary international law, the nine core international human rights treaties and their protocols, as well as the treaties of the three regional human rights mechanisms, and the authoritative interpretations of these instruments by mechanisms established thereunder, or otherwise for the purposes of their promotion and

With some notable exceptions (such as the obligation to make all acts of torture a criminal offence and the prohibition of retroactive criminal offences),[92] international human rights law has not traditionally specified directly what should, or should not, be a criminal offence in national law.[93] Nonetheless, international human rights law jurisprudence increasingly faces the question of whether the criminalization of certain conduct is compatible with, or even required, by individual human rights. In doing so, international human rights law can act both as a 'shield' and a 'sword' – either neutralizing or triggering the criminal law.[94]

While the state which is party to human rights treaties has a obligation to establish criminal law and systems sufficient to deter and respond to attacks on individuals,[95] it must not go so far as to deny individual rights by its criminalization of particular conduct.[96] In undertaking this assessment, the criminal law provision must be assessed on a 'right-by-right' basis,[97] In order to test whether its contents infringe a range of individual rights – such as the right not to be subjected to arbitrary or unlawful interference with privacy, family, home or correspondence,[98] the right to freedom of thought, conscience and religion,[99] or the right of peaceful assembly.[100]

The balancing act

Such an assessment frequently requires international human rights bodies to carefully weigh a number of interests. Many provisions of international human rights law are not absolute. Rights to freedom of thought, conscience, religion, expression, and association, for example, may be subject to restrictions (including criminal law restrictions)[101] that can be shown to be necessary for a range of interests, including national security, public safety, public order, the protection of public health or morals, or the protection of the rights and freedoms of others.[102]

Permissible interferences with human rights must usually be: (i) prescribed by or in accordance with law; (ii) meet legitimate aims; (iii) and be necessary in a democratic society.[103] In the European context, in determining the question of necessity, the ECtHR considers whether the interference is *proportionate* to an identified 'pressing social need'.[104] The state is granted a 'margin of appreciation' in this respect.[105] The margin is 'context dependent' – in particular with reference to

---

implementation, are taken as the principal expression of 'international human rights law'. Including: ICCPR; ICESCR; ICERD; CEDAW; CAT; CRC; ICRMW; CPED; and CRPD. In addition, Optional Protocols to ICESCR, ICCPR, CEDAW, CRC, CAT, and CRPD cover areas such as the abolition of the death penalty (ICCPR-OP2), the involvement of children in armed conflict (OP-CRC-AC), and the sale of children, child prostitution and child pornography (OP-CRC-SC) (also listed as a 'cybercrime' instrument in this Study). At the regional level, including: EHCR and its 15 Protocols, including on protection of property and the right to education, freedom of movement, abolition of the death penalty, and a general prohibition on discrimination, the ACHR in the Americas, and in Africa, the ACHPR. At present, there is no Asia-wide convention on human rights.

92 CAT, Art. 4, and ICCPR, Art. 15(1).

93 It should be noted however that international human rights law does require redress for violations of human rights and that this may imply in turn the promulgation of appropriate criminal laws sufficient to deter and respond to certain violations.

94 Tulkens, F., 2011. The Paradoxical Relationship between Criminal Law and Human Rights. *Journal of International Criminal Justice,* 9(3):577-595.

95 See, for example, ECtHR. Application No 23452/94. 28 October 1998, in which the court stated that the right to life (ECHR, Article 2(1)) included the obligation to put in place *'effective criminal law provisions to deter the commission of offences against the person backed up by law enforcement machinery for the prevention, suppression and sanctioning of breaches of such provisions.'*

96 United Nations Commission on Narcotic Drugs, and Commission on Crime Prevention and Criminal Justice, 2010. *Drug control, crime prevention and criminal justice: A Human Rights perspective.* Note by the Executive Director. E/CN.7/2010/CRP.6 – E/CN.15/2010/CRP.1. 3 March 2010.

97 *Ibid.*

98 ICCPR, Art. 17.

99 ICCPR, Art. 18.

100 ICCPR, Art. 21.

101 The European Court of Human Rights has found that the existence of a criminal prohibition on certain conduct can be sufficient to continuously interfere with human rights (in this case, the right to private life) even where there is a consistent policy of not bringing criminal proceedings. See ECtHR. Application No 15070/89. 22 April 1993.

102 See, for example, ICCPR, Art. 21.

103 See, for example, the formulations used in ECHR, Arts. 8-11.

104 ECtHR. Application No 5493/72. 7 December 1976.

105 For a general review, see Legg, A., 2012. *The Margin of Appreciation in International Human Rights Law.* Oxford: Oxford Monographs in International Law.

the nature of the right involved and the aim that the interference in question is intended to pursue.

Cybercrime – criminal law and human rights

The 'shield' and 'sword' effect of international human rights law applies equally to the criminalization of cybercrime acts. 'Cybercrime' represents a broad area of criminalization – including acts against the confidentiality, integrity and availability of computer data or systems, computer-related acts for personal or financial gain or harm, and computer content-related acts. Some of these criminal provisions may engage international human rights law obligations to a greater extent than others.

Computer *content*-related crimes, in particular, may engage treaty-based rights such as the right to freedom of expression,[106] property-related rights,[107] and the positive obligations of states to ensure security of the person and protection from physical harm.[108] Content available on the internet is, in principle, subject to the same human rights regime as traditional media, such as printed matter and speech. Resolution 20/8 of the United Nations Human Rights Council affirms that the '*same rights that people have offline must also be protected online, in particular freedom of expression, which is applicable regardless of frontiers and through any media of one's choice.*'[109]

Nonetheless, online content has particular features – including the fact that the impact and longevity of information can be multiplied when placed on the internet, that content is easily accessible to minors, and that developments in social media and user-generated internet content have begun to challenge traditional monopolies over information.[110] As a result, the interpretation of human rights provisions must take into account the specific nature of the internet as a means of imparting information.[111]

Cybercrime and the right to freedom of expression

The importance of freedom of expression on the internet has been highlighted by a number of recent high profile cases, as well as by the work of human rights mechanisms at the international and regional level.[112] During information gathering, countries were asked how freedom of expression in electronic form is protected by law, and to specify whether, and under what circumstances, freedom of expression may be restricted for the purposes of preventing or combating cybercrime.

Almost every country that responded to this question (some 50 countries) indicated that freedom of expression in general was protected – usually by constitutional law – and that protection applied equally to electronic and non-electronic expression.[113] A number of countries also referred to laws 'on information', 'press and publications' laws, 'audio-visual' laws, and 'media' laws as

106 ICCPR, Art. 19; ECHR, Art. 9; ACHR, Art. 13; ACHPR, Art. 9.
107 ECHR, Protocol 1, Art. 1; ACHR, Art. 21; ACHPR, Art. 14.
108 ICCPR, Arts. 7 and 17; ECHR, Arts. 3 and 8; ACHR, Arts. 5 and 11; ACHPR, Art. 5.
109 United Nations Human Rights Council, 2012. Resolution 20/8 on *The promotion, protection and enjoyment of human rights on the Internet,* A/HRC/RES/20/8, 16 July 2012.
110 United Nations Human Rights Council, 2012. Summary *of the Human Rights Council panel discussion on the promotion and protection of freedom of expression on the Internet. Report of the Office of the United Nations High Commissioner for Human Rights,* A/HRC/21/30, 2 July 2012.
111 ECtHR, Research Division, 2011. *Internet: Case-law of the European Court of Human Rights.*
112 See, for example, United Nations Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression, and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information. Joint Declaration on Freedom of Expression and the Internet. Available at: http://www.osce.org/fom/78309
113 Study cybercrime questionnaire. Q20.

containing relevant protections.[114]

With respect to limitations on freedom of expression, respondents referred to a wide range of possible restrictions. These included generic limitations found in international human rights law, such as for the protection of 'national security', 'public safety and prevention of disorder or crime,' 'public order,' 'public health,' and 'public morals.' They also included more specific limitations, such as 'breach of confidentiality,' 'legal privilege,' 'defamation,' 'threats to person or property,' 'inducement to crime,' 'material assistance to terrorism,' 'propaganda for war,' 'incitement to genocide,' 'incitement to national, racial or religious hatred,' 'insults to religious feelings,' 'contempt, slander or defamation of protected religions,' 'material jeopardizing harmonious relations amongst peoples, castes, tribes and communities,' 'obscenity,' 'pornography,' 'undermining the prestige of the state or undermining confidence in its financial status,' and 'dissemination of official secrets.'[115]

Freedom of expression on the internet – Case example

In November 2011, the European Court of Justice (ECJ) ruled that ISPs may not be asked to filter content for copyright enforcement purposes, as this would infringe the rights of subscribers to privacy, and to freedom of expression. According to the Court, an injunction to filter would not only 'contravene' the EU Directive on e-Commerce, but it would also '*infring[e] the fundamental rights of [the] ISP's customers, namely their right to protection of their personal data and their freedom to receive or impart information…[Firstly], the injunction requiring installation of the contested filtering system would involve a systematic analysis of all content and the collection and identification of users' IP addresses from which unlawful content on the network is sent. Secondly, that injunction could potentially undermine freedom of information since that system might not distinguish adequately between unlawful content and lawful content, with the result that its introduction could lead to the blocking of lawful communications*'.A management company representing creators of musical works in authorising the use of their copyright-protected materials by third parties, had sued an ISP which provides access to the internet without offering other services such as downloading or file sharing. The former had asked the ISP to monitor and subsequently block P2P transfers of files concerning materials created by European clients it represented.

Source: ECJ Case No. C-70/10

A number of countries referenced international and regional law as the source of some of these limitations, including the EU Council Framework Decision on combating racism and xenophobia,[116] and the Protocol to the Council of Europe Cybercrime Convention.[117] Others referred only to national laws. Some countries provided information on the way in which the legitimacy of limitations is determined.[118] Most countries, however, did not provide information on the approach used to determine the legitimacy of restrictions on freedom of expression. Some countries were clear that specific limitations on freedom of expression arose from criminal prohibitions. In general, however, respondents did not specify whether limitations were of a criminal, administrative or civil nature.

Limitations on freedom of expression and international law

Some limitations on freedom of expression cited by respondents enjoy a high degree of support from international human rights law. At the most extreme, the 'sword' function of international human rights law *requires* prohibition of certain (limited) forms of expression. The

114 *Ibid.*

115 *Ibid.*

116 EU Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law, OJ L 328 of 6 December 2008.

117 Articles 3 to 6 of the Protocol to the Council of Europe Cybercrime Convention require states parties to adopt such legislative and other measures as may be necessary to establish as criminal offences the dissemination of racist and xenophobic material through computer systems, racist and xenophobic motivated threats, racist and xenophobic motivated insults, and denial, gross minimisation, approval or justification of genocide or crimes against humanity.

118 One country in Africa, for example, stated that '*rights in the Bill of Rights may be limited only in terms of law of general application to the extent that the limitation is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors, including – (a) the nature of the right; (b) the importance of the purpose of the limitation; (c) the nature and extent of the limitation; (d) the relation between the limitation and its purpose; and (e) less restrictive means to achieve the purpose.*' Study cybercrime questionnaire. Q20.

United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, identifies four forms of expression that are required to be prohibited by international law: child pornography;[119] direct and public incitement to commit genocide;[120] advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence;[121] and incitement to terrorism.[122] The Special Rapporteur could also have added propaganda for war.[123] As discussed below, other limitations on expression enjoy less support within international human rights law.

The table details a number of human rights provisions and cases, according to outcome – whether criminalization is *required*, *acceptable*, *not required*, or potentially *incompatible* with international human rights law. The table highlights that – at least under the available international jurisprudence – states may legitimately restrict freedom of speech in areas such as hate speech and obscenity. On the other hand, restrictions that are overly broad, that lack legal certainty, or that stifle pluralistic debate may be incompatible with international human rights standards. In this context, international human rights law acts as a *shield* – guarding against over-criminalization.

Criminalization required by international human rights law
ICCPR, Article 20(2), ICERD, Article 4, and ACHR, Article 13 Any advocacy of national, racial or religious hatred that constitutes incitement to [discrimination, hostility or violence (ICCPR)]/[lawless violence or to any other similar action (ACHR)]/[racial discrimination, or to acts of violence against any race or group of persons or another colour or origin (ICERD)] shall be [prohibited by law (ICCPR)] [considered as offences punishable by law (ACHR and ICERD)]
OP-CRC-SC, Article 3 Producing, distributing, disseminating, importing, exporting, offering, selling or possessing for the above purposes child pornography shall be fully covered under criminal or penal law, whether such offences are committed domestically or transnationally or on an individual or organized basis.
ICCPR, Art 20(1) and ACHR, Article 13 Any propaganda for war [shall be prohibited by law (ICCPR)]/[shall be considered as an offence punishable be law (ACHR)]
Criminalization acceptable under human rights decisions
ECtHR Application No 5446/03 A conviction for internet publication of material falling under an obscenity act was found not to breach the right to freedom of expression, even though the material may have been legal in the third country in which the internet site was operated and controlled. The applicant did not dispute that the material was obscene under the Act, and the Court found that the interference was proportionate, taking into account the commercial nature of the internet site.
ECtHR Application No 10883/05 A conviction for incitement to national, racial, or religious discrimination resulting from statements posted by a city mayor on a municipal council website was found not to breach the right to freedom of expression. The statements called for the boycott of products from a third state. The court found the interference to be relevant and sufficient, taking into account the public office held by the applicant.
Criminalization not required under human rights decisions
ECtHR Application No 31358/03 The respondent country was under no obligation to investigate a complaint to the police concerning receipt of unsolicited SPAM containing pornography, where existing criminal laws did not cover such conduct.

Hate speech

At the international level, ICCPR Article 20 provides that '*any advocacy of national, racial or religious hatred that constitute incitement to discrimination, hostility or violence shall be prohibited by law.*'[124] When asked about the criminalization of computer-related acts involving racism or xenophobia, three quarters of responding countries reported that relevant criminal offences existed. The remainder reported that such

119 United Nations OP-CRC-SC, Art. 3.

120 Genocide Convention, Art. 3; Rome Statute, Art. 25(3)(e); Statute of the International Criminal Tribunal for the former Yugoslavia, Art. 4(3)(c); Statute of the International Criminal Tribunal for Rwanda, Art. 2(3)(c).

121 ICCPR, Art. 20(2).

122 United Nations Security Council Resolution 1624 (2005), Para 1.S/RES/1624 (2005), 14 September 2005.

123 ICCPR, Art. 20(1).

124 It should be noted that ICCPR Article 20 does not *require* criminalization, merely prohibition by law. The ACHR and ICERD, on the other hand, require such advocacy to be considered as offences punishable by law.

acts were not a crime.[125]

Where such acts are criminalized, the majority of offences were classified as 'general,' rather than 'cyber-specific.' Approaches to criminalization in this area show considerable diversity. Some countries have offences which cover incitement to racial *and* religious hatred, while others cover only racial or ethnic issues.[126] Positions further range from narrow limitations only on speech intended to 'create fear of future harm,' to broad criminalization covering 'making insulting remarks' about a group of persons on the grounds of race, religion or belief, sex, sexual orientation or disability.[127]

The increasing use of social media has resulted in a number of recent cases involving the internet that raise hate speech issues, including video containing anti-Islamic content and Twitter messages inciting racism.[128] While ICCPR Article 20 imposes an obligation to combat such expression, it is important to recall that ICCPR Article 20 requires a high threshold. Restrictions must meet the three part test of legality, proportionality and necessity. In assessing the severity of the hatred – and hence the justification for restricting freedom of expression – a threshold assessment should include: (i) the context of the statement; (ii) the position or status of the speaker; (iii) the intent (negligence and recklessness should not suffice); (iv) the content or form of statement; (v) the extent of the statement; and (vi) the degree of risk of resulting harm.[129] Non-binding principles

Limits of criminalization under human rights decisions
ECtHR Application No 13290/07 A criminal conviction for defamation of a public official regarding comments posted on a website about decisions of the official was found to be a disproportionate interference with the right to freedom of expression. The Court held that elected officials must have a particular tolerance regarding criticism directed at them and the verbal excesses which may sometimes accompany this.
UN-HRC Communication CCPR/C/103/D/1815/2008 The Committee concluded that the conviction of a radio broadcaster for defamation constituted an illegitimate restriction of the right to freedom of expression. The Committee highlighted that such laws should include the defence of truth and should not be applied to expressions that could not be subject to verification.
ECtHR Application 2034/07 A criminal conviction for 'serious insult against the King' was found to be a disproportionate interference with the right to freedom of expression. The Court noted that such a sanction, by its very nature, will inevitably have a chilling effect.
UN-HRC Communication CCPR/C/85/D/1180/2003 The Committee concluded that the applicant's conviction for criminal insult contained in an article about the leader of a party group was a disproportionate interference with the right to freedom of expression. The Committee noted that for figures in the political domain, the value placed by the Covenant upon uninhibited expression is particularly high.
ECtHR Application 27520/07 A conviction for 'denigrating the nation, the republic, the grand national assembly, and the government of the republic or the judicial bodies of the state' was found to be a disproportionate interference with the right to freedom of expression. The Court observed that the term was too wide and vague and did not enable individuals to regulate their conduct or to foresee the consequences of their acts.
ECtHR Application 35071/97 A conviction for 'incitement to hatred or hostility on the basis of social class, race, religion, denomination or region' regarding comments criticising democratic principles and calling for the introduction of Sharia law was found to be a disproportionate interference with the right to freedom of expression. The Court highlighted that the comments were made in the context of pluralistic debate.

125 Study cybercrime questionnaire. Q35.

126 United Nations Office of the High Commissioner for Human Rights, 2012. *Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.* Conclusions and recommendations emanating from the four regional expert workshops organized by OHCHR, in 2011, and adopted by experts in Rabat, Morocco on 5 October 2012.

127 OSCE, 2011. *Freedom of Expression on the Internet: A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the Internet in OSCE participating States;* and Halpin, S., 2010. Racial hate speech: A comparative analysis of the impact of international human rights law upon the law of the United Kingdom and the United States. *Marquette Law Review,* 94(2):463-497.

128 See, for example, http://www.bbc.co.uk/news/world-middle-east-19606155 and http://www.bbc.co.uk/news/uk-england-gloucestershire-20560496

129 United Nations Office of the High Commissioner for Human Rights, 2012. *Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.* Conclusions and recommendations emanating from the four regional expert workshops organized by OHCHR, in 2011, and adopted by experts in Rabat, Morocco on 5 October 2012.

further highlight that the terms 'hatred' and 'hostility' used in ICCPR Article 20 refer to '*intense and irrational emotions of opprobrium, enmity and detestation towards the target group.*'[130] At the European level, the ECtHR emphasizes the need for genuine and serious incitement to extremism, as opposed to ideas that simply offend, shock or disturb others.[131]

When it comes to 'religious hatred,' in particular, the United Nations Human Rights Committee stresses that prohibitions of displays of 'lack of respect for a religion or other belief system, including blasphemy laws' are incompatible with the ICCPR, except in the specific circumstances envisaged in ICCPR Article 20.[132] The Committee notes, for example, that it would not be permissible for prohibitions to be used to '*prevent or punish criticism of religious leaders or commentary on religious doctrine and tenets of faith.*'[133]

Hate speech: National example from a country in Western Europe

Incitement to hatred
(1) Whosoever, in a manner capable of disturbing the public peace
1. incites hatred against segments of the population or calls for violent or arbitrary measures against them; or
2. assaults the human dignity of others by insulting, maliciously maligning, or defaming segments of the population,
shall be liable to imprisonment from three months to five years.
(2) Whosoever
1. with respect to written materials which incite hatred against segments of the population or a national, racial or religious group, or one characterized by its ethnic customs, which call for violent or arbitrary measures against them, or which assault the human dignity of others by insulting, maliciously maligning or defaming segments of the population or a previously indicated group
(a) disseminates such written materials;
(b) publicly displays, posts, presents, or otherwise makes them accessible;
(c) offers, supplies or makes them accessible to a person under eighteen years; or
(d) produces, obtains, supplies, stocks, offers, announces, commends, undertakes to import or export them, in order to use them or copies obtained from them within the meaning of No.s (a) to (c) or facilitate such use by another; or
2. disseminates a presentation of the content indicated in No 1 above by radio, media services, or telecommunication services
shall be liable to imprisonment not exceeding three years or a fine. …

Incitement to terrorism

A number of instruments at the international and regional level call on states to prohibit incitement to terrorism – using language such as 'public provocation to commit a terrorist offence' or 'incitement to commit a terrorist act.'[134] When asked about the criminalization of terrorism support offences (including computer-related 'incitement to terrorism'), almost 90 per cent of countries reported that relevant offences existed. Where such acts are criminalized, around 80 per cent of countries said that a 'general offence' was used. Only 15 per cent of countries reported the existence of cyber-specific terrorism support offences, with 5 per cent of countries reporting both cyber-specific and general offences.[135]

As with forms of hate speech, the internet and social media create new, broad-reaching platforms for incitement to terrorism.[136] As governments apply existing laws and develop new laws, it is critical – as set out in the UNODC publication on The Use of the Internet for Terrorist Purposes – that states '*strike a sensible balance between the requirements of law enforcement and the protection of*

130 Article 19. 2009. The Camden Principles on Freedom of Expression and Equality. Principle 12.
131 Council of Europe, 2012. *Factsheet – Hate speech.*
132 United Nations Human Rights Committee, 2011. *General Comment No. 34.* Article 19. Freedoms of opinion and expression. CCPR/C/GC/34, 12 September 2011. para. 48.
133 *Ibid.*
134 See, for example, Council of Europe Convention on the Prevention of Terrorism, Art. 5; European Union Council Framework Decision 2002/475/JHA of 13 June 2002 on Combating Terrorism (as amended by Council Framework Decision 2008/919/JHA of 28 November 2008), Art. 3; and United Nations Security Council Resolution 1624 (2005), Para 1.S/RES/1624 (2005), 14 September 2005.
135 Study cybercrime questionnaire. Q38.
136 See, for example, http://www.justice.gov/opa/pr/2011/February/11-nsd-238.html and http://www.cps.gov.uk/news/press_releases/137_07/

human rights and liberties' in this area.[137] Reports submitted by Member States to the United Nations Counter-Terrorism Committee on the implementation of UNSC Resolution 1624 (2005) show considerable diversity in the way in which incitement to terrorism is defined and prohibited in national legislation.[138] In particular, national responses may include or exclude broader acts such as justifying or glorifying terrorist acts.[139]

Incitement to terrorism – Case example

In 2011, a 22-year-old national form a North American country was indicted for his involvement in the distribution of information relating to explosives, and solicitation to commit violence on the country's soil. Additional charges against him included assaulting a law enforcement officer and possessing a firearm in furtherance of a crime of violence. The defendant was an active administrator of an internationally-known, Islamic extremist website, where he placed a number of postings expressing his affinity for radical views while concurrently encouraging other members of his faith to engage in committing crimes of violence in the North American country against such targets as police stations, post offices, synagogues, military facilities, and transportation facilities. In furtherance of such attacks, he also posted a link to a lengthy document containing detailed steps on how to manufacture explosives. The defendant pleaded guilty to soliciting crimes of violence and to possessing a firearm in furtherance of a crime of violence in the summer of 2011, though sentencing has been re-scheduled to January 2013.

From a human rights perspective, the use of vague terms such as 'glorifying' or 'promoting' terrorism may be problematic when restricting expression.[140] The concept of 'glorification', in particular, may not be sufficiently narrow or precise to serve as a basis for criminal sanctions compliant with the requirements of the principle of legality. Rather, incitement can be understood as a direct call to engage in terrorism, with the *intention* that this will promote terrorism, and in a context in which the call is *directly* causally responsible for increasing the actual likelihood of a terrorist act occurring.[141] In particular, the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression proposes that the formulation in UNSC Resolution 1624 (2005) ('Prohibit by law incitement to commit a terrorist act or acts') is best qualified by the position that 'it is an offence to intentionally and unlawfully distribute or otherwise make available a message to the public with the intent to incite the commission of a terrorist offence, where such conduct, whether or not expressly advocating terrorist offences, causes a danger that one or more such offences may be committed.'[142]

Other forms of expression and the challenge of legal traditions and jurisdiction

Other commonly prohibited forms of expression find even less consensus amongst national laws and international and regional approaches. During information gathering for the Study, a number of countries – in all regions of the world – referred to general criminal laws impacting on freedom of expression, including: on libel and insult; on obscenity or pornographic material; on debauchery; on public decency; and on undesirable publications.[143]

As the internet and social media become increasingly important in political activity and socio-cultural expression, there is an emerging need both for (i) national clarifications regarding the

137 UNODC, 2012. *The Use of the Internet for Terrorist Purposes*, p.41.

138 Member state reports on measures in place to prohibit by law and to prevent incitement to commit a terrorist act or acts are Available at: http://www.un.org/en/sc/ctc/resources/1624.html. For an overview, see also van Ginkel, B., 2011. Incitement to Terrorism: A Matter of Prevention or Repression? *ICCT Research Paper*. The Hague: International Centre for Counter-Terrorism,

139 *Ibid.* See, for example, reports submitted by Brazil, Egypt, Latvia, Spain, and United Kingdom of Great Britain and Northern Ireland.

140 United Nations General Assembly, 2008. *The protection of human rights and fundamental freedoms while countering terrorism*. Report of the Secretary-General. A/63/337, 28 August 2008.

141 *Ibid.*

142 United Nations General Assembly, 2011. *Promotion and protection of the right to freedom of opinion and expression*. Report of the Special Rapporteur A/66/290, 10 August 2011.

143 Study cybercrime questionnaire. Q34, Q36 and Q39.

criminal law applicable to forms of online expression; and (ii) discussion concerning criminalization differences arising from jurisdictional issues and diverse legal traditions.

Faced with a large rise in social media 'crimes,'[144] some countries have, for example, recently issued interim guidance on prosecuting cases involving communications sent via social media.[145] Such guidance emphasizes that criminal provisions must be interpreted consistently with free speech principles and can assist in clarifying the extent of acceptable expression. In this respect, the human rights doctrine of the 'margin of appreciation' allows a certain amount of leeway to countries in determining the boundaries of acceptable expression in line with their own cultures and legal traditions.[146] Nonetheless, international human rights law will intervene at a certain point. The United Nations Human Rights Committee has found, for example, that penal defamation laws may breach rights to freedom of expression and should include defences such as the defence of truth.[147] The Committee has also expressed concern regarding laws on matters such as lese majesty, *desacato*, disrespect for authority, disrespect for flags and symbols, defamation of the head of state, and the protection of the honour of public officials.[148]

When it comes to global internet content, cases such as *Perrin*[149] and *LICRA v Yahoo!*[150] highlight difficulties that arise where internet content that is generated and acceptable in one country is made available in a third country. In *Perrin*, for example, the European Court of Human Rights found that application of the obscenity laws of the respondent country to internet content on a site operated and controlled in a third country where the content was not illegal, did not exceed the respondent state's margin of appreciation.[151] Commentators have argued that, in this case, the European Court applied an overly broad margin of appreciation and failed to sufficiently address the jurisdictional issue – potentially sanctioning a wide jurisdictional reach for countries over content producers in other countries, according to their own content standards.[152] The Court did not, for example, examine the closeness or otherwise of the link between the applicant, the site-owning company based in the third country, and the respondent country.[153] In this respect, the Joint

144 In England and Wales, for example, in 2008, there were 556 reports of alleged social media crimes with 46 people charged. In 2012, there were 4,908 reports with 653 people charged. See http://www.bbc.co.uk/news/uk-20851797 In Western Asia, a number of recent criminal cases related to internet social media content have also been reported, see http://www.bbc.co.uk/news/world-middle-east-20587246

145 Crown Prosecution Service, 2012. *Interim guidelines on prosecuting cases involving communications sent via social media.* Issued by the Director of Public Prosecutions, 19 December 2012.

146 Where a particularly important right or value is at stake, the margin of appreciation accorded to a state will, in general, be restricted (ECtHR. Application No 44362/04. 18 April 2006). In contrast, if the aim pursued does not enjoy universal consensus – such as the meaning of the 'protection of morals' – the margin of appreciation will be wide (ECtHR. Application No 10737/84. 24 May 1988). The ECtHR employs, amongst others, a common (European) consensus test in determining the margin available – when consensus on the meaning or need for limitations on particular rights is absent, the margin expands. Conversely, when consensus is present, it is taken to mean that the 'core' meaning of the right is narrowly defined and the margin to deviate contracts. The domestic margin of appreciation thus goes hand in hand with a 'European supervision' – concerning both the aim of interferences and their 'necessity'. The margin of appreciation doctrine is less developed in the work of the Inter-American Court of Human Rights and the United Nations Human Rights Committee. Nonetheless, commentators note that there is an increasing role for the margin of appreciation in the Inter-American system, and that ample evidence supports the proposition that the doctrine forms part of the United Nations Human Rights Committee's practice (Legg, A., 2012. *The Margin of Appreciation in International Human Rights Law.* Oxford: Oxford Monographs in International Law).

147 See United Nations Human Rights Committee Communication CCPR/C/85/D/1180/2003 and United Nations Human Rights Committee, 2011. *General Comment No. 34*. Article 19: Freedoms of opinion and expression. CCPR/C/GC/34, 12 September 2011. para. 47.

148 *Ibid.* para. 38.

149 ECtHR Application No. 5446/04.

150 In *Licra v Yahoo!*, a national court ordered Yahoo! Inc. to take measures to prevent users in that country from accessing an auction web site based in a third country selling Nazi memorabilia (Ordonnance de référérendue le 20 Novembre 2000. Tribunal de grande Instance de Paris. No. RG : 00/05308). In subsequent proceedings in the site-hosting country, a national court held on appeal that there were no grounds for jurisdiction unless or until the foreign court judgement was brought for enforcement in the national courts, and that a freedom of expression argument could not therefore be entertained at that time (*Yahoo Inc. v La Ligue Contre le Racisme et l'Antisemitisme.* No. 01-17424. United States Court of Appeals, Ninth Circuit.)

151 ECtHR Application No. 5446/04.

152 Council of Europe, Commissioner for Human Rights, 2012. *Social Media and Human Rights.* Issue Discussion Paper. CommDH, 8 February 2012.

153 *Ibid.* p.17.

Declaration of the International Mechanisms for Promoting Freedom of Expression on Freedom of Expression and the Internet recommends that jurisdiction in legal cases relating to internet content should be restricted to '*States to which those cases have a real and substantial connection.*' This would be '*normally because the author is established there, the content is uploaded there and/or the content is specifically directed at that State.*'[154]

> *'Prosecutors should have regard to the fact that the context in which interactive social media dialogue takes place is quite different to the context in which other communications take place… Communications intended for a few may reach millions. Against that background, prosecutors should only proceed with cases… where they are satisfied that the communication in question is more than: offensive, shocking or disturbing; or satirical, iconoclastic or rude comment; or the expression of unpopular or unfashionable opinion about serious or trivial matters, or banter or humour, even if distasteful to some or painful to those subjected to it.'*
>
> Guidelines on prosecuting cases involving communications sent via social media (a country in Northern Europe)

Overall, diverse national approaches to the criminalization of internet and social media content can be accommodated by international human rights law, within certain boundaries. These include permissible criminal prohibitions on child pornography; direct and public incitement to commit genocide; advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence; incitement to terrorism; and propaganda for war. Criminal offences relating to defamation, obscene material, and insult, however, will likely face a high threshold – even within the margin of appreciation – of demonstrating that the measures conform to the principle of proportionality, are appropriate to achieve their protective function, and are the least intrusive instrument amongst those which might achieve protection.[155]

Moreover, where states attempt to assert jurisdiction over internet content based on their own national standards, it is likely that international law will increasingly crystallize a need to demonstrate that content created or hosted in other countries is specifically targeted to, or frequently accessed by, persons within the enforcing state. Where content is illegal in one country, but legal to produce and disseminate in another, international human rights law offers an important tool – both as a sword and a shield – in helping to delineate acceptable expression. As international and regional human rights systems develop their jurisprudence, it is possible that, at least in some areas, a human rights 'consensus' can guide the size of the margin of appreciation at the international level. Where national differences ultimately cannot be reconciled, states will likely need to focus criminal justice responses on persons *accessing* content within their national jurisdiction, rather than on content producers *outside* of the national jurisdiction.

---

154 United Nations Special Rapporteur on Freedom of Opinion and Expression, the OSCE Representative on Freedom of the Media, the OAS Special Rapporteur on Freedom of Expression, and the ACHPR Special Rapporteur on Freedom of Expression and Access to Information. Joint Declaration on Freedom of Expression and the Internet. Available at: http://www.osce.org/fom/78309

155 United Nations Human Rights Committee, 2011. *General Comment No. 34.* Article 19: Freedoms of opinion and expression. CCPR/C/GC/34, 12 September 2011. para. 34.

CHAPTER FIVE: LAW ENFORCEMENT AND INVESTIGATIONS

This Chapter examines law enforcement cybercrime investigations from a range of perspectives, including legal powers for investigatory measures, subject privacy safeguards, investigation challenges and good practices, interactions between law enforcement and the private sector, and law enforcement training and capacity. It demonstrates the complexities of cybercrime investigations and the need for effective legal frameworks, combined with law enforcement resources and skills in practice.

5.1 Law enforcement and cybercrime

KEY RESULTS:

- Over 90 per cent of responding countries report that cybercrime acts most frequently come to the attention of law enforcement authorities through reports by individual or corporate victims
- The proportion of actual cybercrime victimization reported to the police ranges upwards from 1 per cent. One global private sector survey suggests that 80 per cent of individual victims of cybercrime do not report to the police
- Law enforcement authorities aim to address underreporting through a range of measures including awareness raising and outreach
- An incident-driven law enforcement response to cybercrime must also be accompanied by medium and long-term strategic investigations that focus on crime markets and criminal scheme architects
- The proportion of cybercrime acts detected through proactive investigations is low, but a number of countries are focusing on undercover strategic operations

The role of law enforcement

Article 1 of the United Nations Code of Conduct for Law Enforcement Officials[1] highlights that the role of law enforcement is to fulfil the duty imposed upon them by law, *'by serving the community*' and '*by protecting all persons against illegal acts*.' This duty extends to the full range of prohibitions under penal statutes.[2] As cybercrime acts become ever more prevalent,[3] law enforcement agencies increasingly face the question of what it means to 'serve' and 'protect' in the context of a crime with global dimensions.

During information gathering for the Study, more than half of countries reported that between 50 and 100 per cent of cybercrime acts encountered by the police involve a *transnational*

1 *Code of Conduct for Law Enforcement Officials*, Art.1. Annex to General Assembly Resolution 34/169, 17 December 1979.
2 *Ibid*., Commentary to Art. 1, at (d).
3 See Chapter Two (The global picture).

element.[4] At the same time, responding countries indicated that the majority of cybercrime acts come to the attention of the police through individual victim reports. Cybercrime thus *occurs globally*, but is *reported locally*. The report may reach a national cybercrime hotline or specialized police unit, but can also reach a municipal or rural police office more accustomed to dealing with 'conventional' burglary, robbery, theft, or homicide. In the same way as 'conventional' crime, however, both 'cyber' victims and 'cyber' perpetrators are real individuals with real geographic locations – both of which fall within a local police jurisdiction.

Local police stations may often transfer cybercrime cases to a specialized national-level law enforcement lead. However, the growing involvement of electronic evidence in *all* crime types is likely to revolutionize policing techniques, both at central *and* local level, in the coming decades. In some countries, for example, local police stations have been routinely equipped with desktop technology for extracting mobile phone data from suspects.[5] Country responses to the Study questionnaire highlight considerable variation in the capacity of police forces to investigate cybercrime both between and within countries. As one country noted: '*The police corps of the localities differ a lot when it comes to cybercrime. Some have well organized cyber units, others barely have a few trained officers.*'[6]

An incident-driven response to cybercrime must, however, be accompanied by medium and long-term strategic investigations that focus on disrupting cybercrime markets and bringing to justice criminal scheme architects. The prevention of *any* form of crime requires a proactive and problem-oriented approach to policing, with police working alongside other multidisciplinary partners[7] towards the overall aim of the maintenance of social order and public safety.[8]

Notions of police 'community' engagement and 'public safety' require some translation in the move from the offline world to the online world. Nonetheless, country responses to the Study questionnaire suggest that this principle, as well as many other elements of police good practice in the prevention of 'conventional' crime, are equally applicable when it comes to cybercrime. These especially include the need for law enforcement agencies to work with private sector and civil society partners, and to apply 'intelligence-led' policing to pre-empt and prevent cybercrime – using problem-solving approaches based on sound information and 'horizon scanning.' As highlighted by one responding country, for example: '*attacks are becoming more and more advanced, more and more difficult to detect and in the same time the techniques quickly find their way to a broader audience.*'[9]

As discussed in this Chapter, critical elements of a consistent law enforcement response to reported acts of cybercrime thus include: (i) an effective legal framework for investigative measures that reaches an appropriate balance between respect for individual privacy and investigative powers; (ii) access to investigative tools and techniques in practice, including means of obtaining electronic evidence from third parties, such as internet service providers; and (iii) sufficient training and technical capabilities both for specialized and non-specialized officers.

---

4 Study cybercrime questionnaire. Q83. Some countries which could not provide exact numbers estimated the percentage to be 'very high.'

5 See http://www.bbc.co.uk/news/technology-18102793

6 Study cybercrime questionnaire. Q113.

7 UNODC. 2010. *Handbook on the Crime Prevention Guidelines: Making them work.*

8 Bowling, B., and Foster, J., 2002. Policing and the Police. *In*: Maguire, M., Morgan, R., Reiner, R. (eds.). *The Oxford Handbook of Criminology*. 3rd edn. Oxford: Oxford University Press.

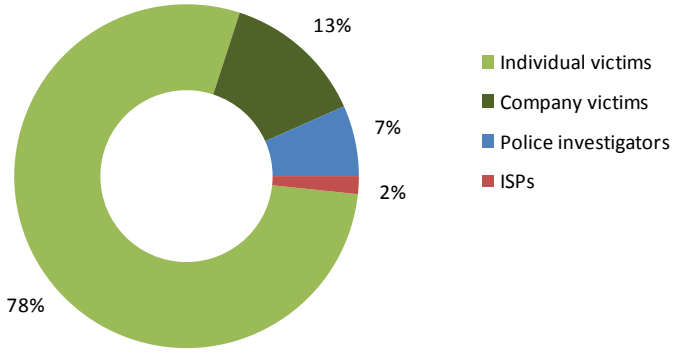
9 Study cybercrime questionnaire. Q85.

What do the police encounter?

During information gathering for the Study, responding countries stated that more than 90 per cent of acts that come to the attention of the police do so through reports from individual and company victims.[10] The remainder of acts were reported to be detected directly by police investigators or obtained from ISP reports.

The picture of cybercrime seen by law enforcement is, as with any crime, necessarily incomplete – being constructed from a mixture of individual investigated cases and broader criminal intelligence. The transnational nature of cybercrime exacerbates the challenge, as investigative leads arrive at overseas servers or IP-addresses, creating delays while formal or informal cooperation mechanisms are engaged.

Figure 5.1: Sources of cybercrime reports to police



Source: Study cybercrime questionnaire. Q78. (n=61)

As noted by one responding country in Africa, for example, '*Most of the crimes, including the unreported ones, involve transnational dimensions. Targets are mostly outside of national boundaries.*'[11] Another country, also in Africa, reported that '*Most of the reported offences are initiated outside this country. In most cases we act as a conduit,*' while one country in Europe highlighted that '*All cybercrime investigations conducted in the last five years have had a transnational dimension. Examples are offences related to use of e-mail accounts, social media and proxy servers.*'[12]

In addition to transnational elements, significant *under*reporting of cybercrime acts in the first place can contribute to a limited picture of the underlying phenomenon. Of the 90 per cent of cybercrime acts that come to the attention of the police through victim reporting, countries estimate that the proportion of *actual* cybercrime victimization reported to the police ranges upwards from only one per cent.[13] One survey conducted by a private sector organization suggests that 80 per cent of individual victims of core cybercrime acts do not report the crime to the police.[14]

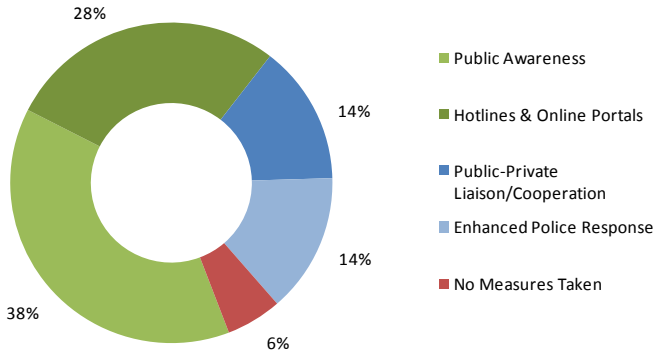
Responding countries to the Study cybercrime questionnaire attributed underreporting of cybercrime acts to a number of factors, including a lack of public confidence in the capacity of police to address cybercrime, a lack of awareness of victimization and of reporting mechanisms, victim shame and embarrassment, and perceived reputation risks for corporations. One country, for example, stated that: '*Estimation is very difficult. Companies and banks are not interested in reporting cybercrimes due to reputational risks.*'[15] Another highlighted that '*Most victims do not even realize that [they] have become targets or the damage done is insignificant enough for them to ignore.*'[16] When cases do come to the attention of the police, subsequent investigation may reveal a much wider pool of victims and offenders than

10 Study cybercrime questionnaire. Q78.
11 Study cybercrime questionnaire. Q83.
12 *Ibid.*
13 Study cybercrime questionnaire. Q82.
14 Symantec. 2012. *Norton Cybercrime Report 2012.*
15 Study cybercrime questionnaire. Q82.
16 *Ibid.*

initially identified at the outset of a case. As noted by one responding country: '*Some of these [crimes] may be more common [than those reported].*'[17]

Many responding countries reported strategies and approaches used to increase reporting of cybercrime. As shown in Figure 5.2 these include the use of public awareness campaigns, creation of online and hotline reporting systems, liaison with private sector organizations, and enhanced police outreach and information sharing. Out of almost 60 responding countries, less than 10 per cent reported not having taken any measures aimed at increasing reporting of cybercrime acts.[18]

Figure 5.2: Measures taken to increase reporting of cybercrime to police



Source: Study cybercrime questionnaire. Q79. (n=57, r=107)

Country responses also showed the need for law enforcement authorities to work closely with other stakeholders, such as the private sector – in order to increase reporting and for intelligence purposes. One country, for example, highlighted that it was important to '*establish 24 hour connectivity between important website administrators, ISPs, police and a centre for coordination of security incidents.*' Another country in the Americas reported that '*The Federal Police is pursuing agreements with public and private companies so that crimes committed against those companies and their clients are informed electronically to the Federal Police.*'[19] Overall, however, the comparatively low proportion of cybercrime acts reported by company victims or internet service providers, suggests that additional outreach and development of public-private partnerships may be needed, in order to strengthen reporting of cybercrime acts from these sources. The development of public-private partnerships and service provider responsibilities is discussed further in Chapter Eight (Prevention). Interactions between law enforcement and third party service providers during police investigations are addressed below in this Chapter.

A notable feature from Figure 5.1 is the low proportion of cybercrime acts that are detected by law enforcement investigators in the absence of victim reports. Accordingly, responding countries did not, in general, refer to proactive investigations in written responses to the questionnaire. One country did, however, note that '*In some cases cybercrime acts come to the attention of the police while police [are] performing operational activities.*'[20] Another country, in Europe, also reported that '*For child pornography offences, the investigations start mostly from information coming from other police forces, and open sources*,' indicating underlying police intelligence work.

The distribution of the source of identified cybercrime acts is indicative, in part, of the challenge of addressing both *strategic* and *tactical* policing objectives. Strategic policing objectives are threat-driven and relate to longer-term law enforcement goals, with a focus on the root causes and circumstances of serious crime. Tactical policing objectives are incident-driven and time-sensitive, with an emphasis on preserving evidence and following investigative leads. In the case of cybercrime, the investment in police time and resources required for responding to individual cases

17 Study cybercrime questionnaire. Q80.
18 Study cybercrime questionnaire. Q79.
19 Study cybercrime questionnaire. Q79.
20 Study cybercrime questionnaire. Q78.

is substantial. As discussed later in this Chapter, many countries highlighted the voluminous amounts of evidence associated with cybercrime investigations and the time consuming nature of investigations into reported cases. One country in the Americas, for example, stated that '*the complexity of cybercrime offences and cybercrime elements of traditional offences has increased significantly, which places additional demands for the training and maintenance of highly-skilled investigators and technical experts, and also increases the amounts of time that need to be spent on individual cases.*'[21] In many countries, law enforcement agency capacity is fully occupied with day-to-day cases. In response to questions on law enforcement capacity for forensic investigations, for example, one country in Africa reported that '*A few forensic examiners/investigators are available at the Federal level, but not enough to serve the whole country. Only one laboratory is functional.*'[22] Another country in the Americas highlighted that '*The challenge is not in the expertise, but the quantity of data that must be analysed.*'[23] The nature of forensic investigations, and law enforcement capacity in this area, is discussed in detail in Chapter Six (Electronic evidence and criminal justice).

In addition to the challenge of capacity and resources, the extent to which proactive cybercrime investigations can be undertaken by law enforcement may also be affected by underlying differences between common and civil law systems regarding prosecutorial and judicial oversight over the initial stages of an investigation,[24] as well as the extent to which intrusive investigative measures can be authorized in intelligence-based or prospective investigations. As discussed in this Chapter, cybercrime investigations often make use of tools, including interception of communications and electronic surveillance, which have the potential to infringe upon privacy-based rights. Countries with international human rights law commitments will need to ensure a proportionate balance between protection of privacy, and infringements for legitimate crime prevention and control purposes. The section below on privacy and investigations examines this area in greater depth.

Nonetheless, law enforcement authorities in developed countries, and also in a number of developing countries, are engaged in medium and long-term strategic investigations. These often involve undercover units targeting offenders on social networking sites, chat rooms, and instant messaging and P2P services. Examples include the infiltration or establishment of online 'carding' forums,[25] the forensic examination of forums used by child pornography offenders,[26] the use of law enforcement officers posing as minors online,[27] and the examination of malware command and control servers.[28] Many of these investigations involve multiple law enforcement agencies and a large range of investigative measures, including those carried out pursuant to judicial authority, such as search or interception orders. Indeed, both strategic and tactical investigations require access to a range of investigative powers, which – in accordance with rule of law principles – must be firmly grounded in legal authority. The next section of this Chapter examines typical cybercrime investigative powers found in international and regional instruments, and in national laws.

21 Study cybercrime questionnaire. Q84.
22 Study cybercrime questionnaire. Q110.
23 *Ibid.*
24 See, for example, INPROL. 2012. *Practitioner's Guide: Common Law and Civil Law Traditions.*
25 See http://www.fbi.gov/news/stories/2008/october/darkmarket_102008 and http://www.fbi.gov/newyork/press-releases/2012/manhattan-u.s.-attorney-and-fbi-assistant-director-in-charge-announce-24-arrests-in-eight-countries-as-part-of-international-cyber-crime-takedown
26 See https://www.europol.europa.eu/sites/default/files/publications/2csefactsheet2012_0.pdf
27 See http://cdrc.jhpolice.gov.in/cyber-crime/
28 See http://www.justice.gov/usao/nys/pressreleases/January13/GoziVirusDocuments/Kuzmin,%20Nikita%20Complaint.pdf

5.2 Investigative powers overview

KEY RESULTS:

- Many countries outside of Europe perceive their national legal frameworks to be insufficient for the investigation of cybercrime
- Overall, national approaches to cybercrime investigative powers show less core commonality than for criminalization
- While legal approaches vary, key investigative powers required include search and seizure, orders for computer data, real-time collection of data, and data preservation
- Across ten investigative measures, countries most often reported the existence of general (non-cyber-specific) powers. A number of countries reported cyber-specific legislation, notably for ensuring expedited preservation of computer data and for obtaining stored subscriber data
- Many countries reported a lack of legal power for advanced investigative measures, such as remote computer forensics

Cyber-specific and general investigative powers

The evidence of cybercrime acts is almost always in electronic, or digital, form. This data can be stored or transient, and can exist in the form of computer files, transmissions, logs, metadata, or network data. Obtaining such evidence requires an amalgamation of traditional and new policing techniques. Law enforcement authorities may use 'traditional' police work (interviewing victims or undercover visual surveillance of suspects) in some stages of an investigation, but require computer-specific approaches for other parts. These can include viewing, and seizing or copying, computer data from devices belonging to suspects; obtaining computer data from third parties such as internet service providers, and – where necessary – intercepting electronic communications.

While some of these investigative actions can be achieved with traditional powers, many procedural provisions do not translate well from a spatial, object-oriented approach to one involving electronic data storage and real-time data flows. In some countries, computer data can be covered by 'traditional' powers of search and seizure of 'anything' believed to be relevant to an offence. Existing 'wiretap' or 'communications interception' laws may also provide sufficient authority for some aspects of cybercrime investigations. In other countries, however, traditional procedural laws might not be capable of being interpreted to include intangible data or IP-based communications. In addition, investigative powers must be able to address challenges such as the volatile nature of electronic evidence, and use of obfuscation techniques by perpetrators – including the use of encryption, proxies, cloud computing service, 'innocent' computer systems infected with malware, and multiple (or 'onion') routing of internet connections.[29] These aspects, in particular,

[29] See, for example, Feigenbaum *et al.*, 2007. A Model of Onion Routing with Provable Anonymity. *Financial Cryptography and Data Security Lecture Notes in Computer Science*, 4886:57-71; and Schwerha, J.J., 2010. *Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers,"* Council of Europe Discussion paper, pp.9-10; Walden, I., 2013. Accessing Data in the Cloud: The Long Arm of the Law Enforcement Agent. *Privacy and Security for Cloud Computing. Computer Communications and*

present particular challenges to traditional powers. Many responding countries reported that investigative powers are frequently '*out of step with new and emerging technologies*' and often '*legislation [is] designed for physical search and search, and therefore the law's instructions…don't feed the needs, interests and constitutional procedures relevant for cybercrime investigations.*'[30]

Legal frameworks for the investigation of cybercrime – whether predominantly 'general' or 'cyber-specific' laws – thus require both: (i) a clear scope of application of the power, in order to guarantee legal certainty in its use; and (ii) sufficient legal authority for actions such as ensuring preservation of computer data, and the collection of stored and real-time data. In this respect, specialized procedural frameworks offer the possibility to clearly define relevant concepts – such as 'computer data' in the first place, as well as data 'at rest' and data 'in transit.'[31] They also allow differentiation between types of data, such as 'subscriber' data (the basic registration details of computer service users, such as name and address), 'traffic' data (data indicating the origin, destination, route, time, date, size, duration, or type of a communication made by means of a computer system), and 'content' data (the actual content of a communication).[32]

During information gathering for the Study, countries were asked about the existence of either general or cyber-specific legal powers for 10 different actions relevant to law enforcement investigations into cybercrime (and other crimes involving electronic evidence). The investigative actions asked about were: (i) law enforcement search for computer hardware or data; (ii) seizure of computer hardware or data; (iii) order to a person for supply to law enforcement of subscriber information; (iv) order to a person for supply of stored traffic data; (v) order to a person for supply for stored content data; (vi) real time collection of traffic data; (vii) real-time collection of content data; (viii) order to a person to preserve and maintain the integrity of computer data under their control for a specified period of time ('expedited preservation' of data); (ix) use of remote computer forensics tools; and (x) direct law enforcement access to extraterritorial computer data ('trans-border' access to computer data).[33]

Figure 5.3: National approaches to investigative measures for cybercrime

Source: Study cybercrime questionnaire. Q42-51. (n=55)

Figure 5.3 provides a broad overview of the existence of legal provisions covering the ten investigative actions, as reported by over 50 country responses to the Study questionnaire. Responses demonstrate that the majority of

Networks 2013, pp.45-71.

30 Study cybercrime questionnaire. Q53.

31 Walden, I., 2003. Addressing the Data Problem. *Information Security Technical Report*, 8(2); Nieman, A., 2009. Cyberforensics: Bridging the Law/Technology Divide. *JILT,* 2009(1).

32 Sieber, U., 2008. Mastering complexity in the global cyberspace: The harmonization of computer-related criminal law. *In*: Delmas-Marty, M., Pieth, M., Sieber, U. (eds.). *Les chemins de l'HarmonisationPénale/Harmonising Criminal Law*. Collection de L'UMR de Droit Comparé de Paris. Paris: Société de législation comparée.

33 See Study cybercrime questionnaire. Q42-51.

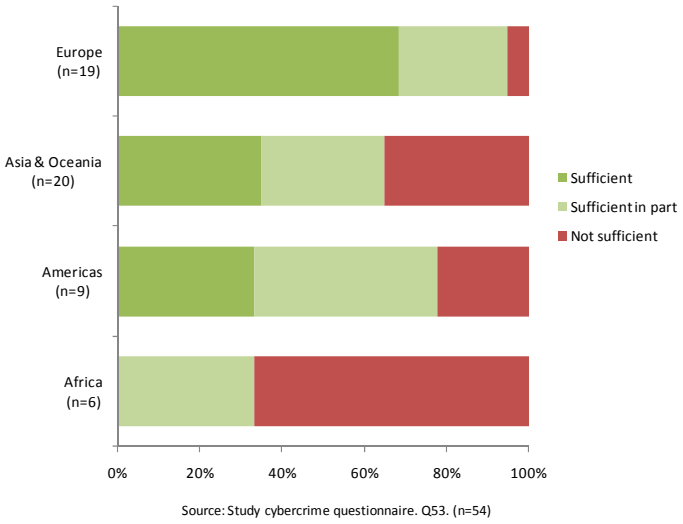
countries rely on *general* legal powers for the investigation of cybercrime. This is the case across a range of investigative actions, including search, seizure, orders for data addressed to third parties, real-time collection of data, and orders for preservation of data. For more intrusive, complex, investigative measures such as remote computer forensics, almost half of responding countries indicated that such measures were not authorized by law. Around 20 per cent of countries reported that no legal power existed for real-time collection of computer data, or for ordering expedited preservation of computer data. Even for basic search and seizure of computer hardware or data, 10 per cent of countries reported that no legal power existed.

Countries that reported the existence of cyber-specific powers showed broad geographic distribution throughout Europe, North and South America, the Caribbean, Western and South-Eastern Asia, the Caribbean, and Northern and Western Africa. Investigative actions most often covered by cyber-specific provisions were orders for subscriber data and for expedited preservation of data – with around 25 to 30 per cent of responding countries reporting the existence of cyber-specific provisions in these areas. The actions of search and seizure for computer hardware and data are most often covered by *both* cyber-specific and general provisions – a situation reported by around 20 per cent of responding countries.

Sufficiency of investigative powers for cybercrime

With respect to the perceived sufficiency of investigative powers, country responses to the Study questionnaire showed a similar pattern to that for criminalization laws. Around 70 per cent of responding countries from Europe reported that investigative powers were sufficient. The remainder viewed investigative powers as sufficient 'in part,' with only one country indicating that powers were insufficient. In other regions of the world, between 20 and 65 per cent of countries reported that investigative powers were insufficient.

Figure 5.4: Sufficiency of national law for cybercrime investigations



Source: Study cybercrime questionnaire. Q53. (n=54)

When asked about the main *gaps* in investigative powers, many countries referred to a lack of power to 'enter' electronic networks in order to search for evidence, as well as a lack of power for preservation of computer data. Countries from Oceania and Europe reported that there was a need for a '*mechanism to expeditiously preserve computer data to support existing search powers*,' and one country in South America highlighted that there was a '*lack of regulation on access to data and connection logs [as well as a] lack of regulation on virtual search possibilities.*'[34]

On the other hand, while many countries reported a complete lack of legal framework specific to cybercrime, a few countries also cited the successful extension of general powers. One country in Southern Africa, for example, reported that '*the Criminal Procedure Act allows the State to seize*

[34] *Ibid.*

anything… [even though] the Act does not provide specifically for cybercrime.'[35] Some countries also reported that it was good practice for powers of investigation relating to computers and other devices to '*extend to all crimes and not just traditional computer crimes*' and that relevant procedural laws should be both '*comprehensive*' and '*precise.*'[36]

Overall, three main approaches were apparent from country responses to the Study questionnaire: Some countries have no specific laws for cybercrime investigations and apply traditional procedural powers as far as possible under a broad interpretation. Other countries have amended general investigatory powers in respect of some specific issues and, through use of general and cyber-specific powers, are able to apply a range of measures such as orders for data, search and seizure of data, and preservation of data. Finally, some countries have introduced a comprehensive range of new investigative powers specifically designed for obtaining electronic evidence. Legislative provisions in one country in Southern Europe, for example, specify four different ways in which data may be considered '*seized*' – (i) seizing the medium itself; (ii) making a copy; (iii) maintaining the integrity of data without removal or copying; and (iv) removing the data or blocking access to the data. Such provisions assist in removing legal uncertainty surrounding the application of 'traditional' investigative powers.

Comprehensive investigative powers for cybercrime: National example from a country in Southern Europe

Seizure of computer data

Seizure of computer data, depending on what is deemed to be most appropriate or proportional, taking into account the interests of the case, may take the following forms:

a) Seizing the computer system support equipment or the computer-data storage medium, as well as devices required to read data;
b) Making a copy of those computer data, in an autonomous means of support, which shall be attached to the file;
c) Maintaining by technological means the integrity of data, without copying or removing them; or
d) Removing the computer data or blocking access thereto.

Examination of the relationship between existence of specialized legislative powers, and the perceived sufficiency of cybercrime investigation frameworks, shows some degree of correspondence for countries that responded to the questionnaire. For those countries that reported investigative frameworks to be 'sufficient' or sufficient 'in part', around 40 per cent of all investigative actions asked about were covered by cyber-specific powers. In contrast, for those countries that reported investigative frameworks to be 'insufficient', only 20 per cent of all investigative actions were covered by cyber-specific powers.[37] This finding highlights the importance of the development of specialized investigative powers – at a minimum, for measures where the extension of traditional powers is in doubt. Chapter Seven (International cooperation) of this Study highlights that the global nature of cybercrime means that a lack of investigative powers in one country can have an impact on other countries where they request international cooperation in the gathering of extraterritorial evidence.

As discussed in Chapter Three (Legislation and frameworks), a number of international and regional instruments provide for comprehensive investigative power frameworks.[38] The table in Annex Three summarizes the powers, by article, in a number of these frameworks. The next section of this Chapter continues to examine, in detail, the nature of investigative power provisions, both as found in multilateral instruments and as reported at the national level through the Study questionnaire. It does so for the powers of: (i) search and seizure; (ii) preservation of computer data;

35 *Ibid.*
36 *Ibid.*
37 Study cybercrime questionnaire. Q42-51 and Q53.
38 See Chapter Three (Legislation and frameworks), Section 3.1 Introduction – The role of law, Relevant categories of law.

(iii) orders for computer data; (iv) real-time collection of computer data; (v) use of remote forensic tools; and (vi) direct law enforcement access to extra-territorial data.

Search and seizure

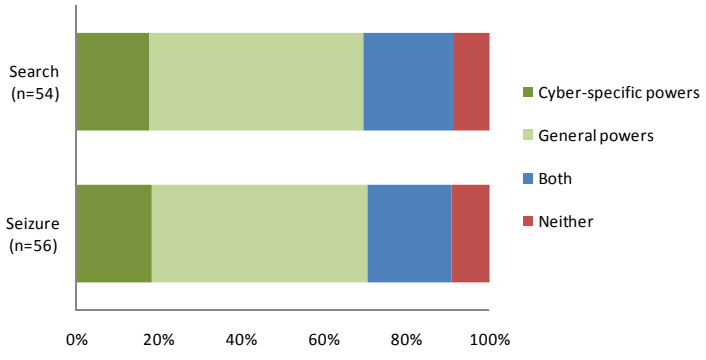
As noted above, countries may face a range of challenges to the extension of 'traditional' search and seizure powers to intangible data.[39] For this reason, seven international or regional cybercrime instruments[40] contain provisions with specific powers to search, or similarly access, computer systems or computer-data storage media. Six of these instruments also provide for an extension of the search to another computer system within the territory of the country, if it is discovered that the information sought after is not in the original system or media searched.[41] A number of multilateral instruments also clarify ways in which computer data can be 'seized.' The Commonwealth Model Law, for example, states that the term 'seized' includes '*taking a printout of output of computer data.*'

Search and seizure warrant: National example from a country in the Americas

(2) A warrant issued under this section may authorize a police officer to:
(a) seize any computer, data, programme, information, document or thing if he reasonably believes that it is evidence that an offence under this Act has been or is about to be committed;
(b) inspect and check the operation of any computer referred to in paragraph *(a)*;
(c) use or cause to be used any computer referred to in paragraph *(a)* to search any programme or data held in or available to such computer;
(d) have access to any information, code or technology which has the capability of transforming or converting an encrypted programme or data held in or available to the computer into readable and comprehensible format or text, for the purpose of investigating any offence under this Act;
(e) convert an encrypted programme or data held in another computer system at the place specified in the warrant, where there are reasonable grounds for believing that computer data connected with the commission of the offence may be stored in that other system;
(f) make and retain a copy of any programme or data held in the computer referred to in paragraph *(a)* or *(e)* and any other programme or data held in the computers.

At the national level, responses to the Study questionnaire showed that search and seizure of computer hardware or data are authorized by *general* criminal procedure laws for the majority of countries (around 50 per cent), rather than by cyber-specific powers.[42] As regards the application of general search powers, one country in Eastern Asia clarified that traditional provisions on searches could also be applied to '*computer*

Figure 5.5: Search and seizure instruments used in cybercrime investigations



Source: Study cybercrime questionnaire. Q42 and Q43. (n=54, 56)

[39] See, for instance, Brenner, S. W., Frederiksen, B.A., 2002. Computer Searches and Seizures: Some Unresolved Issues. *Mich. Telecomm. Tech. L. Rev.* 39(8); Kerr, O.S., 2005. Search Warrants in an Era of Digital Evidence. *Mississippi Law Journal*, 75:85.

[40] Draft African Union Convention, Arts. 3-50, 3-51; COMESA Draft Model Bill, Arts. 37, 33; Commonwealth Model Law, Arts.12, 14; Council of Europe Cybercrime Convention, Art. 19; ECOWAS Draft Directive, Art. 33; ITU/CARICOM/CTU Model Legislative Texts, Art. 20; League of Arab States Convention, Arts. 26, 27.

[41] Draft African Union Convention; COMESA Draft Model Bill; Commonwealth Model Law; Council of Europe Cybercrime Convention; ITU/CARICOM/CTU Model Legislative Texts; League of Arab States Convention.

[42] Study cybercrime questionnaire. Q42 and Q43.

searches', but that the provision only allowed searches for hardware and not of computer data.[43] Less than 20 per cent of responding countries indicated the existence of cyber-specific powers for search or seizure.

Just under 10 per cent of countries reported that there was *no* power at all for search and seizure – at least for computer data. One country from Western Asia, for example, stated that '*In relation to accessing equipment and hardware, the Criminal Procedure Code deals with the case of physical access by members of the judicial police to homes, but does not address electronic crime… These texts do not allow members of the judicial police to enter electronic networks and email on the grounds of suspicion of commission of an offence.*'[44] The same country noted that law reform would be required in order to provide such powers and currently '*If such entry [were to] take place in the absence of a legal provision, that would violate the provisions of the Constitution and the law.*'

Preservation of computer data

Storing computer data requires resources and money. As a result, computer data is typically stored only for the amount of time for which it is needed for processing. In the case, for example, of 'chat' or VOIP content that passes through a service provider's service, this might only be for the amount of time needed for operational purposes, such as the identification of system faults, or customer billing. This could range from a few seconds, to hours, or a few days, or weeks. In addition to the pragmatic cost implications of data storage, many countries also have data protection frameworks that specify that data must not be retained for periods longer than that required by the purposes for which the data are processed.[45] Due legal process requirements, or – in transnational cases – international cooperation requests, may easily take a longer time than the lifespan of the data, before the relevant search warrant or order for supply of stored data can be obtained.[46]

Expedited preservation of data: National example from a country in Southern Africa

Preservation order

(1) Any investigatory authority may apply to the Judge in Chambers for an order for the expeditious preservation of data that has been stored or processed by means of a computer system or any other information and communication technologies, where there are reasonable grounds to believe that such data is vulnerable to loss or modification.
(2) For the purposes of subsection (1), data includes traffic data and subscriber information.
(3) An order made under subsection (1) shall remain in force -
(a) until such time as may reasonably be required for the investigation of an offence;
(b) where prosecution is instituted, until the final determination of the case; or
(c) until such time as the Judge in Chambers deems fit.

As a result, seven international and regional cybercrime instruments contain provisions aimed at establishing mechanisms for preventing the deletion of computer data important to cybercrime investigations.[47] Such actions may be given effect to by an order to a person in control of computer data to preserve and maintain the integrity of the data for a specified period of time, or by expedited procedures for otherwise securing the data, such as through a search and seizure warrant. Key features of typical 'expedited' preservation provisions may include application of a more limited set of

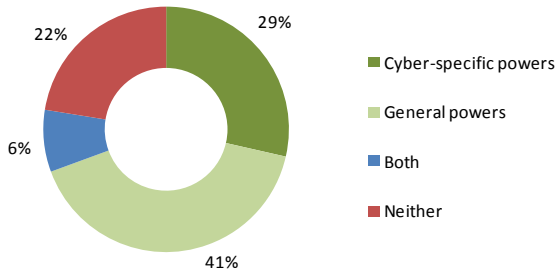
43 *Ibid*
44 Study cybercrime questionnaire. Q53.
45 See Chapter Eight (Prevention), Section 8.3 Cybercrime prevention, the private sector and academia, Cybercrime prevention by internet service and hosting providers.
46 James Tetteh, A.-N., Williams, P., 2008. *Digital forensics and the legal system: A dilemma of our times.* Available at: http://ro.ecu.edu.au/adf/41/
47 Draft African Union Convention, Art. 3-53; COMESA Draft Model Bill, Arts. 33-35; Commonwealth Model Law, Art.17; Council of Europe Cybercrime Convention, Art. 16; ECOWAS Draft Directive, Art. 33; ITU/CARICOM/CTU Model Legislative Texts, Art.23; League of Arab States Convention, Art. 23.

conditions and safeguards than for disclosure of the data, due to an arguably less prejudicial nature of the preservation measure (before the point of any disclosure). In this respect, however, it should be noted that international human rights mechanisms have held that mere storage of information about an individual amounts to an interference with rights to private life.[48] Exercise of preservation orders therefore still requires an assessment of the proportionality of the measure – in particular where compliance with the order would require specific data to be held for longer than the time period envisaged by data protection legislation.

Nonetheless, preservation of data represents an important measure for maintaining vital evidence prior to a full order for disclosure – in particular in the context of transnational investigations. Indeed, the separation of the two obligations, 'preservation' and 'disclosure' is a key element of the measure.[49]

At the national level – perhaps due to the influence of international and regional cybercrime instruments – expedited preservation of data is the measure in respect of which the highest proportion of countries report a cyber-specific power. Nonetheless, country responses also indicated that general provisions could cover the measure in various ways. One country in Western Asia, for example, stated that provisions on search and seizure were interpreted as providing for expedited preservation. Another country in Southern Africa also explained that computer data can be preserved according to its legislation by means of computer seizure, and one country in Western Europe noted that it uses general provisions on seizure of correspondence and other information.[50] In addition, however, over 20 per cent of responding countries indicated that national law did not include a power to ensure expedited preservation of data. The absence of legal authority for such a fundamental investigative tool presents a significant challenge – not only for those particular countries, but also for any other country wishing to seek investigative assistance.

Figure 5.6: Expedited preservation of computer data



Source: Study cybercrime questionnaire. Q49. (n=49)

Orders for computer data

As discussed in Chapter One (Connectivity and cybercrime), a large part of the infrastructure and computer systems used for internet communications are owned and operated by the private sector. Internet service providers, as well as electronic communication providers and web-service providers, therefore route, store, and control a significant amount of computer data related to internet connections, transactions, and content. The use of coercive measures, such as search and seizure, by law enforcement for obtaining these data are unfeasible in the majority of circumstances – due both to the volume of individual cases investigated, and disruption to legitimate business activity. Orders to such third parties to the investigation for computer data thus provide a due legal process route to obtaining electronic evidence.

48 See, for example, ECtHR. Application No. 9248/81.
49 See Brown, I., 2010. Communications Data Retention in an Evolving Internet. *International Journal of Law and Information Technology*, 19(2):107.
50 Study cybercrime questionnaire. Q42-51.

In many countries, such orders may be possible under existing investigative powers, such as general production orders, or document disclosure orders. Nonetheless, procedural challenges can also arise. These could include in respect of 'traditional' requirements for *identifying information* about a suspect before orders for evidence can be made. In cybercrime investigations, at the time of request to an internet service provider, the only known information may be an IP-address or similar connection-based information.

Order for computer data: National example from a country in the Americas

If a magistrate is satisfied on the basis of an application by a police officer that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that-

(a) a person in the territory of <country> in control of a computer produce from the computer specified data or a printout or other intelligible output of that data;

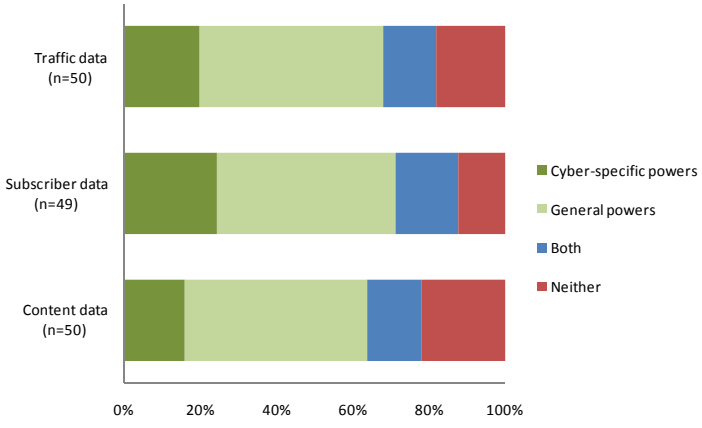
(b) an Internet service provider in <country> produce information about persons who subscribe to or otherwise use the service; or

(c) a person in the territory of <country> who has access to a specified computer process and compile specified computer data from the computer and give it to a specified person

Accordingly, five international or regional cybercrime instruments contain specific provisions regarding orders for obtaining stored data.[51] In doing so, instruments typically refer to the distinction made earlier in this Chapter – between 'subscriber', 'traffic', and 'content' data. Such provisions usually concern information that are in the '*possession or control*' of the person or service provider. The order only applies therefore, to the extent that the data are in existence at the time of the order, and can be retrieved by the subject of the order. The existence of such investigative powers alone does not in itself oblige service providers to collect or retain information they would not otherwise so process. In respect of *traffic* data, some multilateral instruments[52] also include a mechanism for 'partial' expeditious disclosure of sufficient traffic data to enable law authorities to identify the service providers and the path through which the communication was transmitted. This can be important where multiple service providers are involved in processing computer data or electronic communications.

Figure 5.7 shows that at the national level, general powers are again predominant amongst countries for the authorization of orders for subscriber, traffic, and content data.[53] The proportion of countries that employ cyber-specific orders for obtaining subscriber data is slightly higher than for the other two data categories. In addition to the influence of international and regional cybercrime instruments, this may also reflect a common need for this type of data, and a requirement on behalf of service providers for clear legal powers and procedures in requesting

Figure 5.7: Order for stored traffic, subcriber and content data



Source: Study cybercrime questionnaire. Q44, Q45, and Q46. (n=50, 49, 50)

51 COMESA Draft Model Bill, Art. 36(a); Commonwealth Model Law, Art.15; Council of Europe Cybercrime Convention, Art. 18(1)(a); ITU/CARICOM/CTU Model Legislative Texts, Art.22(a); League of Arab States Convention, Art. 25(1).

52 COMESA Draft Model Bill, Art. 34(a)(ii); Commonwealth Model Law, Art.16; Council of Europe Cybercrime Convention, Art. 17(1)(b); ITU/CARICOM/CTU Model Legislative Texts, Art.24; League of Arab States Convention, Art. 24.

53 Study cybercrime questionnaire. Q45-47.

such information.

This is supported by comments from responding countries. One country in the Americas, for example, stated that, although providers often cooperate with law enforcement agencies voluntarily, the application of existing general procedural provisions to orders for supply of data was too onerous and impractical. The country had therefore initiated the process of adopting a cyber-specific provision for subscriber data orders.[54] On the other hand, a few countries reported successful use of general provisions. One country in South-Eastern Asia, for instance, highlighted the possibility of extension of a general investigative power to order '*any document or other thing*.' One country in South America also reported that the power of a judge to '*examine sealed correspondence*' had been extended to stored data.[55]

Order for traffic data: National example from a country in Oceania

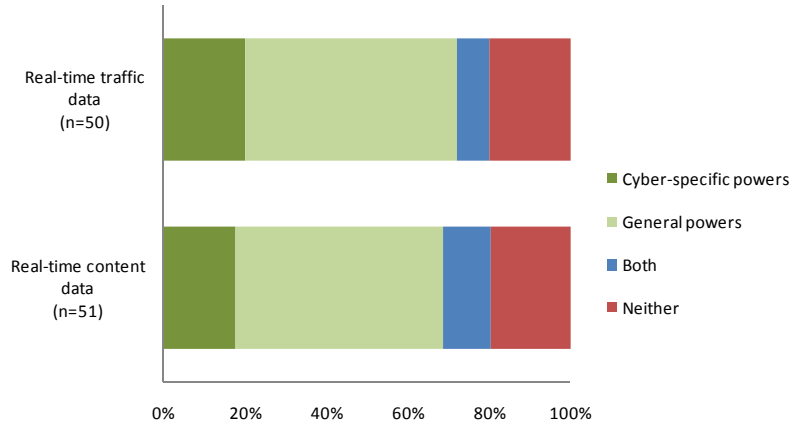
Disclosure of traffic data
Where a magistrate is satisfied on the basis of an application by any police officer that specified data stored in a computer system is reasonably required for the purpose of a criminal investigation or criminal proceedings, the magistrate may order that a person in control of the computer system disclose sufficient traffic data about a specified communication to identify:
(a) the service providers; and
(b) the path through which the communication was transmitted

Aside from the legal form of investigative powers, the interplay between law enforcement and internet service providers for the obtaining of electronic evidence can be particularly complex. Later sections of this Chapter examine the use of powers *in practice*, as well as challenges faced by, and good practice used by, law enforcement in obtaining data from service providers.

Real-time collection of data

Orders for data represent an investigative measure for obtaining *stored* computer data. Crucial electronic evidence may also, however, never be stored at all (existing only in transient communications), or require 'real-time' collection, due to the urgency, sensitivity, or complexity of a law enforcement investigation.

Figure 5.8: Order for real-time traffic and content data



Source: Study cybercrime questionnaire. Q47 and Q48. (n=50, 51).

Accordingly, six international or regional cybercrime instruments include provisions on real-time collection of computer data. In doing so, instruments typically make a distinction between real-time collection of traffic data[56] and of content data.[57] This distinction relates, not least, to differences in the level of intrusiveness into the private life of persons subject to each of the measures.[58] The section on

54 Study cybercrime questionnaire. Q42-51.
55 Study cybercrime questionnaire. Q42-51.
56 COMESA Draft Model Bill, Art. 38; Commonwealth Model Law, Art. 19; Council of Europe Cybercrime Convention, Art. 20; ITU/CARICOM/CTU Model Legislative Texts, Art. 25; League of Arab States Convention, Art. 28.
57 Draft African Union Convention, Art. 3-55; COMESA Draft Model Bill, Art. 39; Commonwealth Model Law, Art. 18; Council of Europe Cybercrime Convention, Art. 21; ITU/CARICOM/CTU Model Legislative Texts, Art.26; League of Arab States Convention, Art. 29.

privacy and investigations in this Chapter examines further possible safeguards that can be required by international human rights law. In this respect, one international instrument, the Council of Europe Cybercrime Convention explicitly refers to interception of content data in relation '*to a range of serious offences to be determined by domestic law*.'[59] From a practical perspective, multilateral instruments often envisage that real-time collection of data can be carried out either directly by law enforcement authorities through the application of their own technical means, or by compelling a service provider, within its existing technical capability, to collect or record computer data, or to co-operate and assist authorities to do so.

At the national level, around 40 per cent of responding countries reported that a general investigative power was used to authorize real-time interception of traffic and content data. A number of countries referred, for example, to the extension of general 'Telecommunications intercept acts' or 'Eavesdropping laws' to the real-time collection of computer data.[60] Overall, more than 60 per cent of responding countries reported the existence of a legal power for real-time collection of data – either through a general or cyber-specific power. Some countries highlighted the application of safeguards to such powers, including the limitation of real-time collection of content data only to serious crimes.[61]

Real-time collection of data: National example from a country in Western Asia

Real-time collection of traffic data

1. If there is a probable cause that a person commits a crime though a computer system, a prosecutor is authorized to file a motion with a court having jurisdiction over the investigation place, to issue an order requesting real-time collection of traffic data, thereby a service provider is obliged to cooperate with and assist an investigative body in real-time collection or recording of traffic data which are associated with specified communications made and transmitted by means of a computer system within the territory...
2. Motions provided by paragraph 1 of the present Article shall consider technical capability for real-time collection and recording of traffic data of the service provider. The term for real time collection and recording of traffic data shall not exceed the term necessary for collecting evidence in criminal case.
3. Motions provided by paragraph 1 and 2 of this Article, shall be considered by the court in accordance with the procedure established by Article <…> of the present Code.

As regards the practicalities of data interception, a distinction is often made between private and public service providers. National legislation in one country in Western Europe, for example, specifies that interception of computer data carried by public providers shall be intercepted with the cooperation of the service provider, unless such cooperation is not possible or is contrary to the interests of the investigation. For non-public service providers, the national legislation providers that the service provider will be '*offered*' the opportunity to cooperate in the interception, unless this is impossible or undesirable.[62]

Remote forensic tools

A range of technological tools offer possibilities to law enforcement agencies both for the direct remote collection of evidence from computer systems, and for the collection of intelligence or investigation-related information more generally. Tools such as key-loggers and remote-administration software, when placed on the device of a suspect, can remotely supply information

58 See Walden, I. *Addressing* the Data Problem: The Legal Framework Governing Forensics in an Online Environment. *Second International Conference iTrust 2004*, Proceedings. Oxford, 29 March-1 April 2004.
59 Council of Europe Cybercrime Convention, Art. 20.
60 Study cybercrime questionnaire. Q47 and Q48.
61 *Ibid.*
62 Koops, B-J. 2010. Cybercrime legislation. *Electronic Journal of Comparative Law*, 14(3).

about keyboard activity and computer data stored on, or transmitted or received, by the device.[63] Due to the range of personal information stored on computer devices, the use of such tools represents a significant intrusion into the private life of investigation subjects. From an evidential perspective, evidence obtained by the use of remote tools on 'live' computer systems may also be open to challenge. It must be demonstrated, for example, that the operations performed by the examiner did not themselves alter the state of the system under investigation.[64]

Remote forensic software: National example from a country in Oceania

Remote access search of thing authorized by warrant

Every person executing a search warrant authorising a remote access search may—

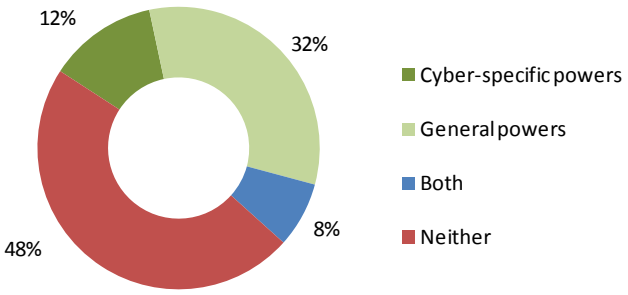
(a) use reasonable measures to gain access to the thing to be searched; and

(b) if any intangible material in the thing is the subject of the search or may otherwise be lawfully seized, copy that material (including by means of previewing, cloning, or other forensic methods).

Only one (non-binding) international or regional instrument refers to the use of remote forensic tools as an investigative measure. The ITU/CARICOM/CTU Model Legislative Text (Art. 27) provides that a judge may authorize a police officer to utilize '*remote forensic software*' for a specific task required for an investigation. More generally, the Council of Europe Child Protection Convention (Art 30(5)) also refers to the obligation to take necessary legislative and other measures in order to allow, where appropriate, for the possibility of '*covert operations*.'

More than one-third of country respondents to the Study questionnaire did not provide an answer regarding the existence of legislation authorizing the use of remote forensic tools in law enforcement investigations. Of those that did, almost half reported that no such power existed. For the other half of respondents that indicated such powers were included in legislation, the majority referred to a general power, rather than a cyber-specific power. Comments provided by countries ranged from explicitly stating that '*there are no legislative provisions for… use of remote forensic tools*', to confirming that national law *'permits the installation of a data surveillance device.*'[65] Other countries commented more generally that procedural frameworks provided, in certain circumstances, for the use of '*technical or scientific expertise*' in order to obtain information required during an investigation.[66]

Figure 5.9: Use of remote forensics tools



Source: Study cybercrime questionnaire. Q50. (n=40)

Direct law enforcement access to extra-territorial data

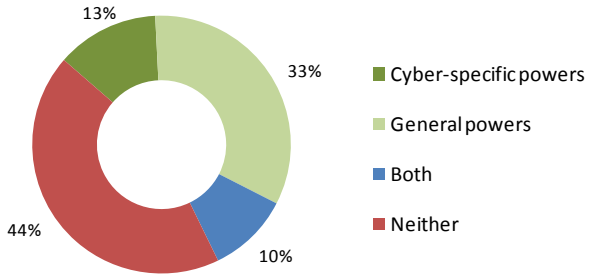
Global connectivity means that computer data relevant to law enforcement investigations – both for cybercrime and crime in general – is increasingly found extraterritorially to the investigating jurisdiction. As discussed in Chapter Seven (International cooperation), traditional formal means of international cooperation may not be sufficiently timely to ensure access to extraterritorial volatile

63 See, for example, Gartner. 2012. *Remote Forensics Report 2012*.
64 Hay, B., Nance, K., Bishop, M. 2009. Live Analysis: Progress and Challenges. *IEEE Security and Privacy*, 7(2):32.
65 Study cybercrime questionnaire. Q42-51.
66 *Ibid.*

data. In recognition of this challenge, three international or regional instruments contain provisions on 'trans-border' access to computer data.[67] Such provisions typically envisage that law enforcement authorities may access or receive, through a computer system in the national territory, stored computer data located in another country, with the lawful and voluntary consent of a person who has lawful authority to disclose the data.[68]

As with remote forensic tools, over one-third of responding countries did not respond to the question in the Study questionnaire on existence of powers for 'trans-border' access. Of those that did, slightly more than half indicated that such a power existed. Countries interpreted the term widely, however, to also include the situation where consent to the measure is obtained from the authorities of the country in which the measure is implemented. One country, for example, reported that legislation allows for the issue of a warrant permitting the installation of surveillance devices in '*overseas premises/objects.*' However, this can only be done where a '*judge… issuing the warrant is satisfied that the surveillance has been agreed to by an 'appropriate consenting official' of the foreign country.*'[69] Some countries that indicated 'trans-border' access powers in national law, referred in written comments to the use of mutual legal assistance instruments. Thus, the overall proportion of countries reporting legislative authority for 'trans-border' access through the Study questionnaire, may be larger than the group of countries with the power to authorize 'trans-border' access in the stricter sense (ie. without authorization from national authorities) envisaged by some international and regional instruments.

Figure 5.10: Trans-border access to a computer system or data



Source: Study cybercrime questionnaire. Q51. (n=39)

Chapter Seven (International cooperation) examines issues of direct law enforcement access to extraterritorial data in greater depth – including with reference to police use of such measures in practice.

Discussion

Examination of the legal basis for investigative powers used in cybercrime (and, indeed, for any crime involving electronic evidence) reveals considerable diversity in approach at national level. This includes regarding the extent to which 'traditional' powers can be interpreted to apply to non-tangible data, as well as the extent to which legal authority exists for particularly intrusive measures, such as remote forensic investigations. Overall, national approaches to cybercrime investigative powers show less core commonality than for criminalization of many cybercrime acts. Nonetheless, while legal powers vary, a good degree of consensus appears to exist on the *types* of investigative measure that *should* be available. These are comparatively straight forward and correspond to those found in many multilateral instruments – (i) powers for search and seizure; (ii) powers for obtaining

67 See COMESA Draft Model Bill, Art. 49b; Council of Europe Cybercrime Convention, Art. 32b; League of Arab States Convention, Art. 40(2).

68 'Trans-border' access provisons typically distinguish between access to publicly available (open source) material and other material. Access to open source material for criminal justice purposes has become generally accepted practice (See Council of Europe. 2012. *Transborder access and jurisdiction: what are the options? Report of the Transborder Group Adopted by the T-CY on 6 December 2012*). Use of the term 'Trans-border' access in this Study therefore concerns access to non-open source material.

69 Study cybercrime questionnaire. Q42-51.

stored computer data; (iii) powers for real-time collection of data; and (iv) powers for ensuring expedited preservation of data.

In addition to the legal basis of such powers, two further issues require consideration – (a) the limits and safeguards that should be applied to such powers; and (b) the use of investigative powers in practice. The next section of this Chapter examines limits and safeguards through the lens of international human rights standards on privacy. Subsequent sections of the Chapter consider use of investigative measures in practice.

5.3 Privacy and investigative measures

KEY RESULTS:

- Almost all responding countries report that privacy-based protections are applicable in the context of computer data and electronic communications
- Countries report the existence of a wide range of safeguards for the protection of privacy during law enforcement investigations, including restrictions on data that can be accessed, time limits, 'probable cause' requirements, and prosecutorial and judicial oversight
- International human rights law sets out clear protections for the privacy rights of persons subject to law enforcement investigations. Core principles include that investigative powers must give a clear indication of the conditions and circumstances under which measures may be used, together with effective guarantees against abuse
- The development of cloud computing introduces a high degree of uncertainty for users concerning the privacy regime that will apply to their data, and the circumstances under which privacy may legitimately be infringed for the purposes of law enforcement investigations or security surveillance

Human rights and law enforcement investigations

International human rights law has a specific concern for the *manner* in which the state achieves its crime prevention and criminal justice goals.[70] All aspects of the investigation and prosecution of crime have the potential to engage human rights standards, and criminal *procedure* law and practice therefore come under particular scrutiny from international human rights law. [71]

A range of rights potentially apply to law enforcement investigations – including rights to liberty and security of person, and rights to fair trial.[72] Often, however, challenges in this area are founded on *privacy*-based protections within international and national law. All of the ICCPR, ECHR and ACHR contain prohibitions on arbitrary interference with privacy, family, home and correspondence.[73] The scope of 'privacy' under international law is broad[74] and case law is clear that the intrusive nature of criminal investigations will engage privacy-based rights[75] – including where a

70 United Nations Commission on Narcotic Drugs and Commission on Crime Prevention and Criminal Justice. 2010. *Drug control, crime prevention and criminal justice: A Human Rights perspective*. Note by the Executive Director. E/CN.7/2010/CRP.6 – E/CN.15/2010/CRP.1., 3 March 2010.

71 Colvin, M., and Cooper, J. (eds.) 2009. *Human Rights in the Investigation and Prosecution of Crime*. Oxford: Oxford University Press.

72 ICCPR, Arts. 9 and 14.

73 ICCPR, Art. 17; ECHR, Art. 8; ACHR, Art. 11.

74 See for example, United Nations Human Rights Committee. 1988. *General Comment No. 16: The right to respect of privacy, family, home and correspondence, and protection of honour and reputation*, 8 April 1998.

75 See for example, United Nations Human Rights Committee. *Communication CCPR/C/82/D/903/1999*; IACtHR *Tristán Donoso*. Judgement of 27 January 2009; and ECtHR Application No's 35394/97 and 13710/88.

suspect is unaware that information is being collected,[76] and even where the mere existence of legislation providing for investigative powers entails such a threat.[77]

As with a number of other rights, privacy rights in international law are not absolute and are subject to limitations – including, in the case of the ECHR, specifically for '*the prevention of disorder or crime*.'[78] In this respect, safeguards in criminal procedure law such as the definition of the conditions and circumstances under which investigative powers can be used; the identity of authorizing officials; the manner of authorization; and the length of time investigative measures may be applied, are critical to the human rights assessment of whether criminal investigations that infringe privacy are acceptable as lawful and necessary.[79]

When it comes to the investigation of cybercrime, each investigative measure must be assessed in its own legal and practical context, in order to determine whether its interference with the privacy, family, home or correspondence of its subject is justified. While the often covert and/or electronic surveillance nature of cybercrime investigative techniques may raise particular privacy challenges,[80] it is important to remember that the proportionality requirements of privacy rights apply equally to 'simple' search and seizure measures.[81] Procedural law limits and safeguards must therefore reflect the varying intrusiveness of investigative measures – ensuring that each measure is only used as necessary in a democratic society.

Existence of privacy protections and procedural safeguards

During information gathering for the Study, countries responded to questions about the legal protection of privacy in the context of computer data or electronic communication and about how privacy rights function as safeguards during law enforcement investigations. Countries were also asked under what circumstances privacy rights may be restricted for the purposes of detecting and investigating cybercrime, and about extra-jurisdictional and international cooperation-related elements of privacy rights.

Almost all responding countries indicated that privacy protections applied in the context of computer data and electronic communications. The way in which such protections are enshrined in law, however, showed considerable differences. Many countries referred to generic constitutional privacy rights which were also applied to computer data. A few countries even highlighted the 'technologically neutral' approach of privacy rights in their national law. Others cited specific legislation, including 'privacy' acts; 'privacy protection' laws; 'telecommunications regulatory' acts; 'protection of privacy in electronic communications' acts; 'criminal code' offences on invasion of privacy; 'search and surveillance' acts; 'confidentiality of correspondence' laws; and 'communications secrets acts.'[82] Some countries referenced international instruments, such as the ECHR, as sources of national privacy protections. A few countries stated explicitly that they had no 'general' privacy

---

76 See ECtHR Application No. 8691/79.

77 See ECtHR Application No. 54934/00.

78 See, for example, EHCR Article 8(2) which provides that '*There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.*'

79 The general approach adopted by the United Nations Human Rights Committee is to ask whether an interference with privacy is provided for by law, is in accordance with the provisions, aims and objectives of the Covenant and is reasonable in the particular circumstances of the case (See United Nations Human Rights Committee. *Communication CCPR/C/82/D/903/1999* and Human Rights Committee. *General Comment No. 16*.) The approach of the ECtHR in law enforcement investigations cases is to ask (i) whether there was an interference with the privacy rights protected by Article 8 ECHR; (ii) whether the interference was in accordance with law – including not only the basis in domestic law but also the 'quality' of the law, in terms of its accessibility, foreseeability and compatibility with the rule of law; and (iii) whether the interference was necessary in a democratic society (See ECtHR Application No. 62540/00).

80 See for example, UNODC. 2009. *Current practices in electronic surveillance in the investigation of serious and organized crime*.

81 See for example, ECtHR Application No. 13710/88.

82 Study cybercrime questionnaire. Q21.

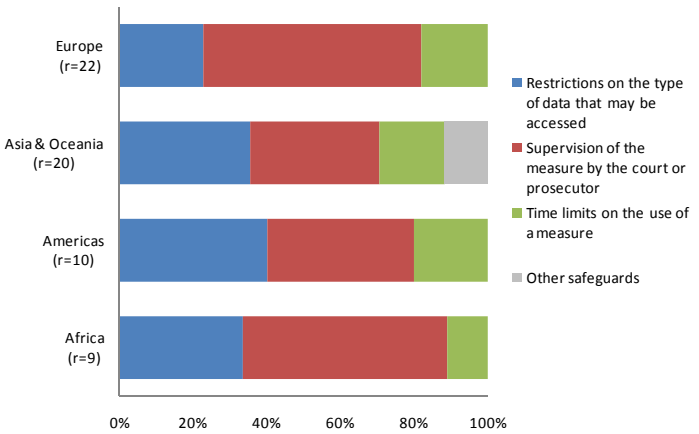
law. Nonetheless, computer data and electronic communications in these countries was reported to benefit from protections such as confidentiality and legal professional privilege laws.[83]

A number of countries confirmed that privacy protections were applicable in the context of law enforcement investigations, but highlighted that privacy had to be balanced against the need to prevent and investigate crime. While some countries described how this balance was achieved, the majority of countries referred only to the requirements for warrants or judicial or prosecutorial authority for intrusive searches or monitoring. One country highlighted that national law specified that '*due care shall be exercised [during search and seizure] in order to prevent the disclosure of private circumstances not connected with the criminal proceedings.*'[84] Another noted that wiretapping of communications must be used only as a '*supplementary*' means of facilitating a criminal investigation. Some countries highlighted, in particular, that data protection laws (which function as an important means of protecting privacy in the context of personal data controlled and processed by third parties) contained exclusions allowing, for example, third parties to disclose information to a law enforcement agency where 'reasonably necessary' for the enforcement of criminal law.[85]

Further detail about the nature of procedural safeguards that help secure human rights and respect for privacy during the investigative process was also requested by the Study questionnaire from law enforcement officials. In response to this question, the majority of states (85 per cent) specified that national limits and safeguards existed for law enforcement investigative cybercrime measures.[86] Surprisingly, therefore, a few countries stated that safeguards did *not* exist – a situation which may lead to incompatibility with international human rights law.

Reported safeguards included restrictions on the types of computer data that may be accessed by law enforcement, as well as supervision of investigative measures by the court or prosecutor. Some states also referred to time limits placed on the use of investigative measures.[87] Other countries cited protective regimes including limitations on access to computer data once acquired by law enforcement, limitations on its use, destruction requirements, and internal and independent oversight mechanisms.[88] One country reported that '*A wide variety of limits and safeguards apply, with different limitations and safeguard regimes being applied to each access*

Figure 5.11: Limits and safeguards on investigations



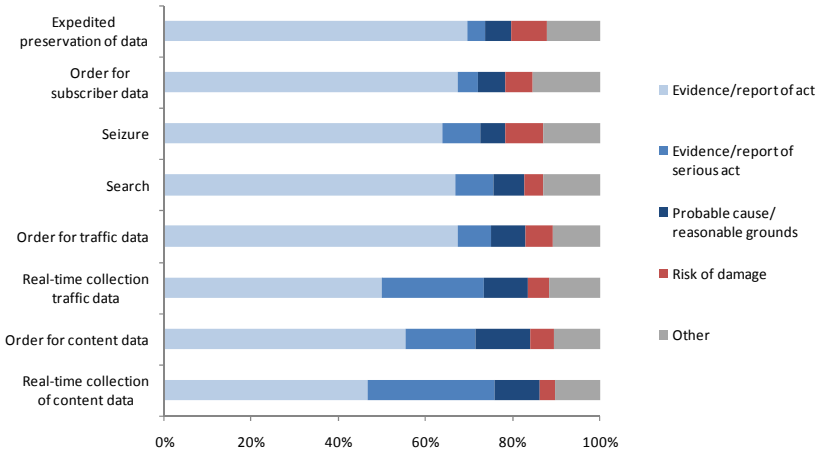
Source: Study cybercrime questionnaire Q100. (n=45, r=61)

83 *Ibid.*
84 *Ibid.*
85 *Ibid.*
86 Study cybercrime questionnaire. Q100.
87 *Ibid.*
88 *Ibid.* It should be noted, in addition, that countries in the European Union are subject to Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, which regulates the processing of personal data by such authorities.

power (telecommunications data, stored content and live content). These regimes include requirements that must be met before access is granted, limitations on access once granted, limitations of the use of material once accessed, destruction requirements, internal and independent oversight regimes, and public reporting requirements.'[89]

The majority of countries (over 75 per cent), said that safeguards were build into primary legislation. The remainder of countries reported that safeguards derived from secondary legislation, executive decree, court decisions or law enforcement of prosecution policies.[90] While safeguards might legitimately derive from sources other than primary legislation, they must still – as discussed below – be enshrined in 'law' that provides adequate and effective guarantees against abuse of the investigative measure itself.

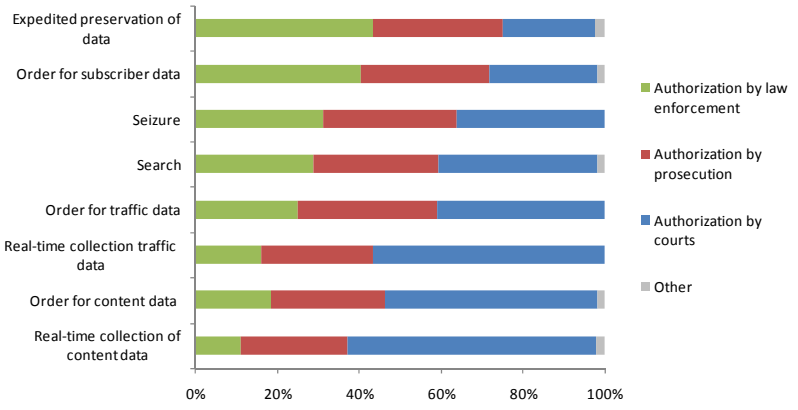
Figure 5.12: Legal requirements for use of investigative measures



Source: Study cybercrime questionnaire. Q87-96. (n=51)

Countries were also asked further detail about specific procedural safeguards. These included the nature of legal requirements to be met before a particular investigative measure could be used, as well as the identity of authorizing authorities. With respect to procedural requirements, the majority of countries reported that a large range of investigative measures could be initiated on the basis of '*evidence or report of a [cybercrime] act.*'[91] For measures with a higher degree of intrusiveness, such as real-time collection of data, or collection of content data, countries more often required evidence or report of a '*serious*' cybercrime, or procedural requirements such as demonstration of '*probable cause*' or '*reasonable grounds*' of suspicion of an offence.[92]

Figure 5.13: Authorization of investigative measures



Source: Study cybercrime questionnaire. Q87-96. (n=51)

A similar pattern was observed with respect to the identity of the authorizing authority for different investigative measures. Countries frequently reported that comparatively less intrusive measures, such as expedited preservation of data, or orders for subscriber data, could be

89 Study cybercrime questionnaire. Q100.
90 *Ibid.*
91 Study cybercrime questionnaire. Q87-96.
92 *Ibid.*

ordered by law enforcement authorities, as compared with more intrusive measures.[93] Over 80 per cent of responding countries, for example, stated that intrusive measures such as orders for content data or real-time collection of data, required authorization by a prosecutor or by the courts, rather than directly by law enforcement officers. Nonetheless, a small number of countries reported that law enforcement authorities were able to authorize such investigations – raising potential concerns over the sufficiency of safeguards for these measures. One country in the Americas, for example, reported that an article of its procedural law, which had provided for interception in exceptional circumstances without a warrant, had been declared unconstitutional by the Supreme Court.[94]

Assessing safeguards through a human rights lens

Case law from international human rights courts and tribunals emphasizes that procedural protections are critical to respecting privacy in the context of law enforcement investigations. The table shows the core international right to privacy provisions, as well as human rights decisions related to issues such as the absence of authorizing legislation for investigative measures; legislative safeguards; and the use of investigative measures in practice. To date, few international human rights decisions have directly addressed law enforcement cybercrime investigations.[95]

One important judgement of the ECtHR has, however, considered the balance of privacy and law enforcement investigations. In the context of an online content offence involving a minor, law enforcement agencies were unable to obtain subscriber data from an ISP due to confidentiality protections contained in the telecommunications law. The Court found that this prevented effective steps from being taken to identify and prosecute the perpetrator.[96]

> *Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime… It is the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context.*
>
> ECtHR Application No. 2872/02

International human rights law provisions
ICCPR, Article 17, ECHR Article 8, ACHR Article 11 [No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence (ICCPR)] [Everyone has the right to respect for his private and family life, his home and his correspondence (ECHR)] [No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence (ACHR)]
Absence of authorizing legislation for investigative measures
ECtHR Application No. 8691/79 In the absence of legal rules, the practice of voluntary supply by a telecommunications service provider of records of telephone numbers dialled and call duration, upon request, to police when 'essential for police enquiries and in relation to serious crime' was found to be incompatible with the right to privacy. The Court highlighted the absence of legal rules concerning the scope and manner of exercise of the discretion.
ECtHR Application No. 47114/99 The interception of pager messages by law enforcement using a 'clone' of a suspect's personal pager in the absence of laws regulating the interception of page messages was found to be incompatible with the right to privacy. The Court noted that domestic law must provide protection against arbitrary interference with the right to privacy.

93 *Ibid.*
94 *Ibid.*
95 Although the ECtHR, for example, has considered the monitoring of email and internet usage in an employment context. See ECtHR Application No. 62617/00. In this case, the Court applied the tests of identifying whether there was an interference with privacy and (finding so), whether the interference was in accordance with the law.
96 ECtHR Application No. 2872/02.

A number of other decisions are also particularly relevant to the cybercrime investigative context. In the European system, the voluntary supply of telephone records by a telecommunications service provider to law enforcement, for example, has been found to be incompatible with the right to privacy in the absence of specific legal rules.[97] Similarly, in the Americas, the recording of telephone conversations authorized by mere judicial annotation and not linked with an established investigation has been found to violate the right to privacy.[98]

It is very likely that existing principles from such cases will be applied in future cybercrime cases. The search of a computer system for files, or the covert monitoring of emails or IP traffic, for example, shows close parallels with traditional physical search and wiretaps. The actions of ISPs in delivering data to law enforcement authorities (whether under an informal cooperation agreement, or pursuant to a warrant, subpoena or other legal order) are equivalent to those of telecommunication providers. In particular, the potential for cybercrime investigations to access a wide range of personal information – including emails, VOIP calls, internet browsing histories, and photographs – presents a particularly high level of potential intrusiveness. In many cases, such as when records are requested from an ISP or real-time data collection is authorized, the subject of the investigation will likely be unaware of the fact of the investigation and of the nature and extent of data gathered, thus engaging human rights jurisprudence on secret surveillance.[99] In such circumstances – due, not least, to resultant vulnerabilities to misuse – regional human rights tribunals have urged particular caution.[100]

Legislative safeguards for investigative measures
UN-HRC Communication CCPR/C/82/D/903/1999 The interception and recording of data traffic on the written authorization of an investigating judge, in the context of a preliminary judicial investigation into the involvement of an individual in a criminal organization, was found not to violate the right to privacy. The Committee highlighted that authorizing legislation detailed the precise circumstances in which interference may be permitted and that the interference was proportionate and necessary to achieve the legitimate purpose of combating crime.
ECtHR Application No. 2872/02 The lack of an effective criminal investigation due to the absence of an explicit legal provision authorizing the disclosure of telecommunications data in the case of an online content offence was found to be incompatible with the positive obligations of the right to privacy. The Court highlighted that the victim had not been afforded effective protection.
ECtHR Application No. 62540/00 The provisions of a national law regulating secret surveillance measures were found to be incompatible with the right to privacy. The Court emphasized that the law did not provide for any review of implementation of measures by an external body or official; that it did not set out procedures for preservation of the integrity and confidentiality of evidence obtained, or procedures for its destruction; and that overall control of surveillance rested with a member of the executive, rather than an independent body.
Investigative measures in practice
IACtHR *Escher* Judgment of 6 July 2009 The recording of telephone conversations by the state and their subsequent dissemination without full respect for national legal requirements was found to be incompatible with the right to privacy. The Court emphasized that the monitoring petition was not linked to an established police investigation or criminal proceeding. The Court also highlighted that the interception was authorized by a mere judicial annotation that did not demonstrate reasoning, procedural requirements, or duration of the measure.
ECtHR Application No. 13710/88 A search impinging on the profession secrecy of a lawyer's office under a broad warrant authorizing search for and seizure of 'documents' was found to be incompatible with the right to privacy. The Court held that the measure was not proportionate to its aims.

97 ECtHR Application No. 8691/79
98 IACtHR *Escher* Judgement of 6 July 2009.
99 In addition to cases in the table, see also ECtHR Application No. 54934/00.
100 The ECtHR holds, for instance, that '*Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the*

The range of privacy and safeguard approaches reported by countries through the Study questionnaire – and, indeed, the range of situations brought before international human rights tribunals – demonstrates a considerable diversity in privacy protection during law enforcement investigations. Examination of relevant *national* privacy decisions further highlights this point. National decisions on the procedure for law enforcement access to ISP subscriber information, for example, range from those which hold that police requests to ISPs for subscriber information *without* judicial authorization are *compatible* with customer privacy expectations, to those which hold that proper judicial process is *required* by privacy rights. [101]

As with a human rights assessment of criminalization, international human rights law is, to some extent, able to accommodate such differences through doctrine such as the margin of appreciation.[102] Nonetheless, it is clear that divergent national privacy approaches will become an increasing challenge in the context of trans-national law enforcement investigations and developments such as cloud computing.

Privacy, jurisdiction and the cloud

Cloud data processing involves multiple data locales or data centres, distributed across different national jurisdictions, and with different private data controllers and processors.[103] Under present conditions, although data location may be technically knowable, cloud computing users are not always informed exactly 'where' their data is held. In turn, jurisdictional approaches both to the *data protection* regime governing data held by cloud service providers, and *criminal procedure law* governing national law enforcement investigations are complex.[104]

This introduces a high degree of uncertainty for users concerning the privacy regime that will apply to their data and the circumstances under which privacy may be infringed for the purposes of law enforcement investigations or security surveillance. Legislation in some countries, for example, contains extensive surveillance powers that could apply, without judicial authorization, to the data of non-nationals which is 'at rest' in cloud servers located within the national jurisdiction.[105] Where national privacy guarantees differentiate between nationals and non-nationals,[106] users may have (i) no knowledge of such actions; and (ii) no legal recourse, either under the law of the state applying such investigative measures, or – depending upon the jurisdictional application of their home laws (and the legal incorporation structure of the cloud service provider) – within their own countries.

Divergences in privacy law jurisdiction are suggested by country responses to the Study questionnaire. Responding countries reported a range of legal positions regarding the extra-territorial application of national privacy protections. A few countries noted that privacy protections do have extra-territorial effect, including under conditions such as where the act or practice falling outside of the territory nonetheless has an '*organisational link*' with the country. Other countries confirmed that national privacy laws do not apply to computer data or electronic communications, either in real-time or stored outside of the territory. One country stated that it was an '*open question, whether computer material located abroad would enjoy the same [privacy] protection as computer material located in a server [within the*

Convention only in so far as strictly necessary for safeguarding the democratic institutions.' ECtHR Application No. 28341/95.

101 See for example, *R v Ward*, 2012 ONCA 660 and *State v. Reid*, 194 N.J. 376 (2008).

102 Legg, A., 2012. *The Margin of Appreciation in International Human Rights Law*. Oxford: Oxford Monographs in International Law.

103 On the concepts of data 'controllers' and 'processors', see Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (as amended by Regulation (EC) No. 1882/2003 of the European Parliament and of the Council of 29 September 2003).

104 See, for example European Parliament Directorate General for Internal Polices, Citizens' Rights and Constitutional Affairs. 2012. *Fighting cybercrime and protecting privacy in the cloud.*

105 *Ibid.*

106 See for example, *Verdugo-Urquidez* 494 U.S. 259 (1990) and USFISCR No. 08-01.

territory].'[107] The majority of responding countries were nonetheless clear that national privacy protections would apply to investigative actions carried out within the territory at the request of foreign law enforcement. One country noted, for example that '*when a request for mutual legal assistance by a foreign country intrudes upon the domestic law which protects privacy, such request can be set aside*.'[108]

Recent work by the European Parliament finds that '*in the field of cybercrime, the challenge of privacy in a cloud context is underestimated, if not ignored*.'[109] While countries may have developed a range of privacy safeguards for law enforcement action within a national context, these are diverse and may not be easily reconciled in trans-national cybercrime investigation situations – potentially leading to conflicts of laws or jurisdictional gaps. As countries work to promulgate laws that address the delicate balance between individual privacy and the prevention and control of crime, it is critical that national laws reflect common rule of law and human rights principles for law enforcement investigative actions.

One strong starting point can be found in the human rights jurisprudence discussed above and summarized in the box below – which sets out clear rule of law principles for surveillance laws. Even such principles, however, have yet to grapple with the challenging questions of cross-territorial data transfers. In this respect, while harmonization of privacy standards will help to increase the predictability of law enforcement access to user data, including by foreign authorities, countries will also increasingly need to address the jurisdictional reach of national privacy protections. This may entail both: (i) ensuring that support to foreign law enforcement investigations is fully subject to national privacy standards; and (ii) that causes of action are available to persons outside of national jurisdictions that are affected by the actions of the law enforcement authorities of that country.

Rule of law principles for surveillance laws

- Law must be sufficiently clear to give an adequate indication of conditions and circumstances in which authorities are empowered to use an investigative measure, including:
  - The nature of the offences which may give rise to use of the measure
  - A definition of the categories of people liable to the measure
  - A limit on the duration of the measure
  - The procedure to be followed for examining, using and storing the data obtained
  - Precautions to be taken when communicating the data to other parties
  - The circumstances in which data obtained may or must be erased or destroyed
- Adequate and effective guarantees must exist against abuse, taking into account:
  - The nature, scope and duration of the possible measures
  - The grounds required for ordering them
  - The authorities competent to permit, carry out and supervise them
  - Remedies provided in national law
- Laws should provide for review or oversight of implementation of measures by a body or official that is either external to the services deploying the measure or having certain qualifications ensuring its independence
- Laws should provide that as soon as notification can be made without jeopardising the purpose of the measure after its termination, information should be provided to the persons concerned

ECtHR Application No. 62540/00

107 Study cybercrime questionnaire. Q21.
108 *Ibid.*
109 European Parliament Directorate General for Internal Policies, Citizens' Rights and Constitutional Affairs. 2012. *Fighting cybercrime and protecting privacy in the cloud.*

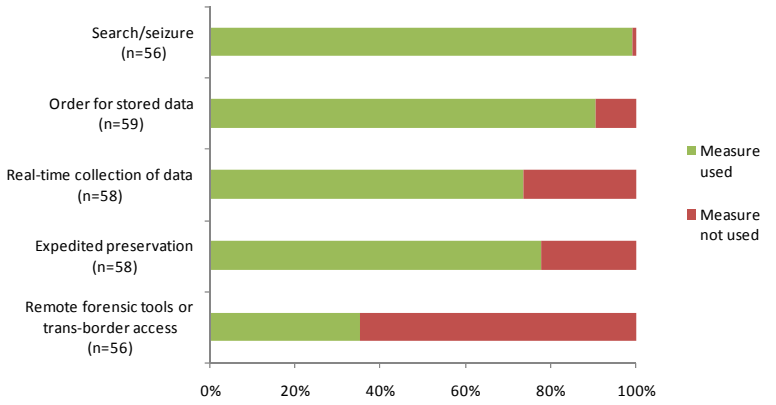
5.4 Use of investigative measures in practice

KEY RESULTS:

- Irrespective of the legal form of investigative powers, all responding countries use search and seizure for the physical appropriation of computer equipment and the capture of computer data
- The majority of countries also use orders for obtaining computer data from internet service providers, real-time collection of data, and expedited preservation of data
- Law enforcement authorities encounter a range of challenges in practice, including perpetrator techniques for hiding or deletion of computer data related to an offence

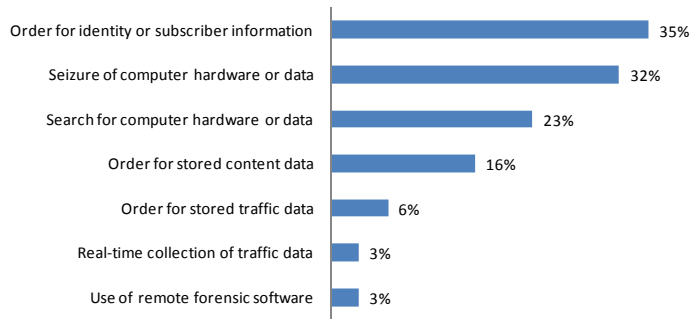
Irrespective of the legal form of powers, law enforcement respondents to the Study questionnaire indicated that a range of investigative measures – from search and seizure, to expedited preservation of data – are widely used in practice. Almost all countries, for example, reported using search and seizure for the physical appropriation of computer equipment and the capture of computer data. Responses from law enforcement officers also suggested that more than 90 per cent of countries made use of orders for obtaining stored computer data. Around 80 per cent of respondents reported making use of expedited preservation of data.[110] Corresponding with the low proportion of countries reporting relevant legal powers, less than 40 per cent of countries reported making use of remote forensic tools or 'trans-border' access.[111]

Figure 5.14: Use of investigative measures by law enforcement



Source: Study cybercrime questionnaire. Q87-97. (n= 56, 59, 58)

Figure 5.15: Most commonly used investigative measures



Source: Study cybercrime questionnaire. Q98. (n=31, r=37)

While these responses fit broadly with the reported existence of legal powers, expedited preservation was reported to be used *in practice* somewhat more frequently than responses on the existence of *legal powers* suggested.[112] This

110 Study cybercrime questionnaire. Q87-96.
111 Study cybercrime questionnaire. Q87-96.
112 See above, Section 5.2 Investigative powers overview.

may be indicative of expedited preservation of data in practice through *informal* working relationships between law enforcement and service providers.

Country responses regarding the *most commonly* used investigative powers also highlighted the importance of search and seizure, as well as the use of orders to obtain subscriber data from service providers. As more and more devices become connected to the internet, computer data that may previously have been stored only on a local computer device is increasingly processed by private sector service providers, including in cloud services. The importance for law enforcement officers of obtaining electronic evidence from service providers is reflected in the fact that orders for subscriber information are reported to be the most commonly used investigative measure. The section below on investigations and the private sector examines law enforcement and service provider interactions in detail.

Investigative challenges and good practice

Responding countries identified a number of challenges and good practices related to the use of investigative measures and cybercrime investigations in general. Good practices reported by countries frequently highlighted the importance of careful organization and ordering of investigations. One country, for example, reported that '*Preservation of data, and seizure of stored data and computer data in a forensically sound manner is a baseline for successful cybercrime investigations*.'[113] Another stated that '*All actions should be recorded and leave an auditable trail. Each action, URL, e-mail address, etc., should be timed and dated, information sources and contacts recorded*.'[114] In addition, a number of countries noted that the starting point for successful investigations is frequently information such as an IP address. As a result, it was considered good practice to focus on ensuring the capability for timely obtaining of subscriber information.[115]

With respect to investigative challenges encountered, many responding countries opened their remarks on law enforcement cybercrime investigations by highlighting an increasing level of criminal sophistication, and the need for law enforcement investigations to 'keep up' with cybercrime perpetrators. One country from Europe, for example, noted that '*attacks are becoming more and more advanced, more and more difficult to detect, and at the same time the techniques quickly find their way to a broader audience… we've also seen that digital components (as means, crime scene or target) become of more and more importance in basically every crime*.'[116] Another country emphasized that '*increases in the incidence of cybercrime offences are being driven by the advancement of technical and programmatic tools available to attackers underpinned by an illicit market for the commercialization of tools for committing cybercrime*.'[117]

Increasing levels of sophistication bring increased challenges in areas such as locating electronic evidence; use of obfuscation techniques by perpetrators; challenges with large volumes of data for analysis; and challenges with obtaining data from service providers. At a basic investigative level, for example, digital storage and connectivity are increasingly integrated into common household and personal items, such as pens, cameras, watches with flash storage and USB jewellery flash drives. In addition, wireless storage devices may be hidden in wall cavities, ceilings and floor spaces. As noted by one country, such physical (and electronic) '*ease of concealment*' of computer data can present difficulties for investigations.[118] Countries also highlighted problems of '*deletion of data storage devices*.' Where perpetrators use online communication services, such as VOIP, computer data

113 Study cybercrime questionnaire. Q99.
114 *Ibid.*
115 *Ibid.*
116 Study cybercrime questionnaire. Q85.
117 Study cybercrime questionnaire. Q84.
118 Study cybercrime questionnaire. Q87-96.

may flow directly from user to user (and not through service provider servers),[119] meaning that only local copies of certain data are available – and vulnerable to subsequent deletion. In addition, perpetrators may make use of 'dead-dropping' of messages in draft folders of webmail accounts (allowing communication without a 'sent' email), combined with use of free public Wifi access points, or pre-paid mobile and credit cards. One country, for example, highlighted challenges in '*pinpointing location*' due to '*availability of numerous free access points.*'[120] Many countries also reported the use of encryption and obfuscation techniques by perpetrators. This area is address in detail in Chapter Six (Electronic evidence and criminal justice).

Finally, many countries noted that significant challenges were faced in obtaining information from service providers. One country in the Americas, for example, reported that the supply of subscriber information by internet service providers on a voluntary basis led to inconsistent practice across the country.[121] Other countries reported that service providers did not store computer data for '*long enough*', and that it '*takes too much time for the subscriber to provide the data to the police.*'[122] A country in Asia further reported the challenge of '*inaccurate registration details*' stored by service providers.[123] The interactions – both formal and informal – between law enforcement and service providers are examined in the next section of this Chapter.

5.5 Investigations and the private sector

KEY RESULTS:

- The interplay between law enforcement and internet service providers is particularly complex. Service providers can hold subscriber information, billing invoices, some connection logs, location information, and communication content
- National legal obligations and private sector data retention and disclosure polices vary widely by country, industry and type of data. Some countries report challenges in obtaining data from service providers
- Service providers most commonly report requiring due legal process for disclosure of customer data. Accordingly, countries most often report using court orders to obtain electronic evidence from service providers
- In some cases, however, law enforcement may be able to obtain data directly. This can be facilitated by informal partnerships between law enforcement authorities and service providers

Obtaining data from service providers

Country and private sector responses to the Study questionnaire represent a mixed and complex picture concerning interactions between law enforcement and the private sector. This picture is characterized by: (i) differences between countries in legal powers to order release of computer data by service providers; (ii) challenges where service providers are located extraterritorially; and (iii) differences in private sector policies and degrees of formal and informal cooperation with law enforcement authorities.

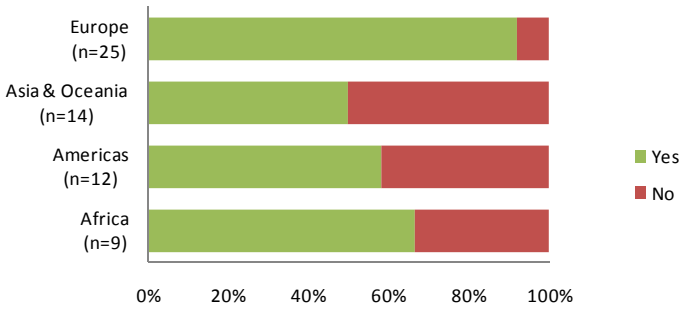
119 See, for example, http://blogs.skype.com/en/2012/07/what_does_skypes_architecture_do.html
120 Study cybercrime questionnaire. Q87-96
121 *Ibid.*
122 *Ibid.*
123 *Ibid.*

Electronic service providers hold subscriber information, billing invoices, some connection logs, location information (such as cell tower data for mobile providers), and communication content, all of which can represent critical electronic evidence of an offence. Electronic service providers are generally not, however, obliged to affirmatively report criminal activity on their networks to law enforcement, (although in several countries, the identification of child pornography engages a mandatory reporting obligation). As a result, responding countries make use of legal powers to obtain computer data from service providers that is required in the course of a criminal investigation. As discussed above, the majority of responding countries reported the existence of general or cyber-specific powers for ordering supply of data from third parties such as service providers.

Responding countries stated, for example, that '*According to Criminal Procedure Law, a person directing proceedings authorized by prosecutor… can demand necessary retained data that could be related to the crime committed.*'[124] Countries also noted that *'police can ask persons and companies to testify as witnesses, hand over data or do anything else that could help the case.*'[125] Nonetheless, responding country comments indicated that a number of countries either still do not have sufficient legislative powers, or experience challenges in *practice* in obtaining data.[126] A common reported issue was that internet service providers are frequently not under any obligation to retain computer data, and that by the time necessary orders had been authorized, connection logs were no longer available.[127] A number of countries also highlighted challenges in resolving privacy issues related to the supply of data by service providers.[128]

Such challenges were more frequently reported in countries outside of Europe. This pattern is also confirmed by law enforcement responses to a question on the ability to compel non-targets of an investigation to provide information. Figure 5.16 shows that only around 60 per cent of countries in Africa, Asia and Oceania, and the Americas reported that this was possible. Almost all countries in Europe, on the other hand, report the ability to compel the production of information from third parties. This information represents the law enforcement 'practical' perspective, in contrast to the earlier data presented in this Chapter on existence of 'legal' power in principle.

Figure 5.16: Law enforcement compel non-targets to provide information



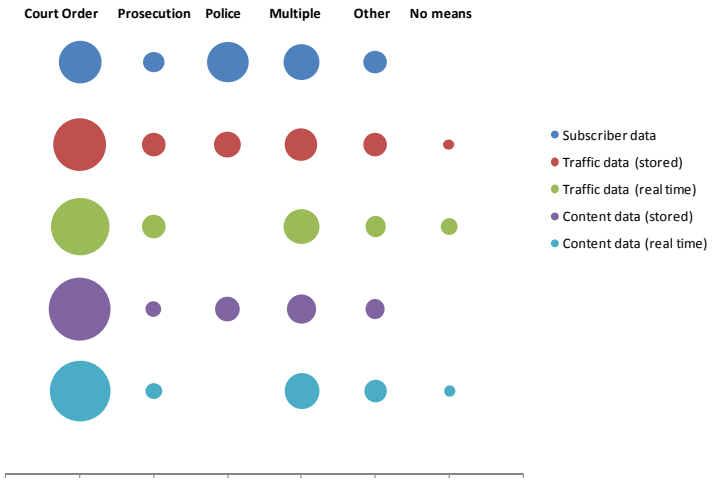
Source: Study cybercrime questionnaire. Q101. (n=60)

In practice, law enforcement officers most often reported using formal court orders in order to obtain computer data from service providers. Figure 5.17 shows the relative distribution of responses for methods used to obtain subscriber data, stored traffic and content data, and real-time traffic and content data. As might be expected from its least intrusive nature, methods used to obtain subscriber data were most diverse – including all of orders issued by courts, prosecution, and police.

124 Study cybercrime questionnaire. Q101.
125 *Ibid.*
126 Study cybercrime questionnaire. Q89-91.
127 *Ibid.*
128 *Ibid.*

A number of countries reported that multiple means of obtaining data were available, depending upon a number of factors, including the stage of investigation or proceedings, and the urgency of the request. One country in Western Asia, for example reported that stored content data could be obtained from a service provider '*Based on the order of the public prosecutor during the process of investigation… or on the order of the court during the trial process.*'[129] Another country noted that subscriber data could be obtained on the basis of a '*Prosecutor order, or in case of emergency, a police letter with formal agreement of the prosecutor.*'[130] 'Other' means for obtaining data were also referred to. One country, for example, highlighted simplified means of obtaining subscriber data, through '*accessing the Integrated Public Number Database which is a database of subscriber information managed by a large carrier pursuant to legislation.*'[131] Overall, responses showed significant diversity in means employed by States, including police requests, 'formal' requests, legal notices, warrants, judicial orders, and subpoenas.

Figure 5.17: Practical and legal procedures to obtain information and evidence from service providers



Source: Cybercrime study questionnaire. Q102. (n=58)

Obtaining data from service providers: National example from a country in the Americas

Federal legislation from one country in the Americas provides that a government entity may require the disclosure by a provider of an electronic communication service of the contents of a wire or electronic communication that is in electronic storage in an electronic communications system for one hundred and eight days or less, only pursuant to a warrant. Under this legislation, domestic law enforcement may obtain access to some types of data through a subpoena (issued usually by a prosecutor), but require a court-issued warrant in order to obtain other forms of data.

Email communication	Authorization procedure
In remote storage, opened	Subpoena
In remote storage, unopened and stored for more than 180 days	
In transit	Warrant
In storage on home computer	
In remote storage, unopened and stored for 180 days or less	

The national legislation also contains provisions compelling an ISP to disclose customer communications in '*exigent circumstances*.' Several national laws also permit the disclosure of communications content and non-content to a governmental entity, if the provider, in good faith believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

Law enforcement officials may also issue a letter to a service provider to order preservation of records and other evidence in its possession pending the issuance of a court order or other process for up to 90 days. Non-compliance with such an order is generally confined to civil remedies and fines against the company.

129 Study cybercrime questionnaire. Q102.
130 *Ibid.*
131 *Ibid.*

Private sector perspectives

Information gathering for the Study also included the collection of information from private sector organizations regarding perspectives on, and experience of, cooperation with law enforcement authorities. Private sector organizations that completed the Study questionnaire reported a range of internal polices and external obligations concerning domestic and foreign law enforcement data requests. In addition, many private sector polices are publicly available in the form of 'law enforcement handbooks' that provide guidance on data retention polices and frameworks for law enforcement requests.[132]

In response to the Study questionnaire, many law enforcement authorities highlighted challenges regarding short data retention times by private sector organizations and service providers.[133] With a view to providing information on retention practice, the table below provides information from a sample of private sector retention and law enforcement access policies. The table demonstrates that a range of data are generated and stored during the provision of computing and electronic communication services. It also shows divergent data retention policies for these different types of data – giving a strong indication of the challenges faced by law enforcement and private sector organizations in identifying and securing appropriate information for use in evidence. None of the service providers reviewed, for example, retained identical information for identical time periods. Publicly available retention periods ranged from as little as one day to indefinitely. Some information appeared to only be retained during the period in which the subscriber account remained active. A number of private sector organizations indicated that responding to law enforcement requests can be time-consuming and not always easily accomplished due to storage and records retention protocols and policies. The availability of sufficient personnel to respond requests may also hamper compliance or its timeliness. For smaller organizations, compliance with law enforcement requests appears to be more burdensome in terms of expenditures of personnel and resources.[134]

Private sector organization data storage and retention

Company	Types of data produced	Data retention period	Requirement of a formal request for disclosure
Communication and Information Services Provider #1	Chat room dialogue	None	Yes
	Instant messenger conversations		
	Member directory logs		
	Email IP/connection access logs	60 days	
	Group IP logs		
	Internet connection access logs		
	TV phone (ANI) connection logs		
Communication and Information Services Provider	IP connection history records	60 days	Yes
	Transactional data	90 days (Private)/60 days (Groups)	

132 See, for example, https://www.facebook.com/safety/groups/law/guidelines/ ; http://pages.ebay.com/securitycenter/LawEnforcementCenter.html ; http://support.twitter.com/articles/41949-guidelines-for-law-enforcement# ; and http://myspace.desk.com/customer/portal/articles/526170-law-enforcement-support

133 See Chapter Eight (Prevention), Section 8.3 Cybercrime prevention, the private sector and academia, Cybercrime prevention by internet service and hosting providers.

134 Study cybercrime interviews (private sector).

#2	Email account registration records	As long as account exists	
	Game account		
	ID records		
Communication and Information Services #3	Web mail account information	Different retention periods	Yes
	IP address log files	180 days	
	Account records	Minimum 2 years	
	Call detail records		
Communication Services Provider	Instant messaging	30-90 days	Yes
	Video message content		
	Voicemail		
	Financial transactions	As long as necessary	
	Registration data		
	Service and account information		
Game Developer and Network Provider	Private user communications	Different retention periods (up to 180 days)	Yes
	Account information	Indefinitely	
	IP logs		
Information and Services Provider #1	Domains	Different retention periods (1 day to indefinite)	Yes
	Email		
	Proxy IP connection logs	5-7 days	
	Member IP connection logs	90 days	
	Source IP connection logs		
	Session logs	6 months	
Information and Services Provider #2	Domains/web-hosting activity logs and content	Minimum of 30 days after termination of Group/website/domain	Yes
	Group content and activity log		
	Chat/Instant messenger logs	45-60 days	
	Email	4 or more months of inactivity	
	Subscriber information	18 months after inactivity	
	Account content	90 days after deletion of account	
	Profiles		
	Account log-in IP addresses	Up to one year	
Messaging Service Provider	Subscriber information	Different retention periods	Yes
	Account content Links, cookies Location information Log data Widget data	Up to 37 days after account deletion	
Social Network Provider #1	Registration data (User Basic Subscriber Information)	Up to 90 days after account deletion	Yes
	Transactional data (IP Logs)		
Social Network Provider #2	Private user communications	Different retention periods	Yes
	Basic user identity information, general records	As long as account exists/10 days after account deletion	
	IP address logs	90 days	

The overriding concern of corporations with respect to law enforcement requests appeared to be that of being able to supply data where requested, but '*without infringing on the scope of other*

legislative or regulatory requirements.'[135] Private sector organizations referred frequently to customer terms of service use, and to privacy considerations. Nonetheless, private sector organizations highlighted, in particular, that they should respond rapidly and positively where '*life is at risk*', but also noted that '*is very, very rare*.'[136] Responding private sector organizations, including service providers, drew a clear distinction between formal legal requirements to provide data, and informal requests. Almost all responding corporations reported that they '*must'* and '*do*' respond to formal domestic court orders to produce information '*according to applicable laws*'[137] and '*in accordance with our legal responsibilities*.'[138] Upon receiving a request, for example, one private sector organization reported that the first step is to identify '*if there is an underlying statutory right to request the information or there is a statutory disclosure obligation to provide information and to seek to ensure we do not violate any other laws or company's contractual obligations to clients' and customer privacy*.'[139]

The majority of private sector organizations reported that they did not consider themselves to be under any obligation to provide data in response to an 'informal' request – such as a telephone call – from law enforcement authorities. Although a number of organizations reported that they may choose to provide data voluntary to informal requests in accordance with their own internal polices. One international corporation noted, for example that it could respond to such requests '*if the data is available and providing it is in accordance with company legal and human resource regulations*.'[140] A larger number of organizations reported that they could provide data in response to a 'formal' law enforcement request – such as an official letter. Almost all, however, indicated that this was not an absolute obligation and data could only be provided under certain conditions, such as where '*there is a statutory obligation to provide information and the disclosure does not violate other laws or company contractual obligations*.'[141]

International corporations and national service providers frequently reported the appointment of law enforcement focal points in order to facilitate cooperation with law enforcement authorities. These included in-house CSIRT, IT security, legal, risk management, or security departments. Other companies have cross-disciplinary teams or task forces to manage relationships with law enforcement. Some private sector organizations reported that mechanisms for strengthening cooperation and information exchange with law enforcement were still in the course of development.[142] Such mechanisms were viewed as important in light of an increasing number of law enforcement requests for data from service providers. One multinational telecommunications operator, for example, reported a 50-fold increase in the number of formal requests for computer data received between the years 2008 and 2010.[143]

Private sector organizations also highlighted the fact that they often received both *domestic* and *foreign* law enforcement requests. Many corporations reported that they only considered *foreign* law enforcement requests where made through *formal national* channels.[144] Some corporations, stated, for example, that foreign law enforcement authorities are required to obtain an order for data from a national court, through a mutual legal assistance request. Corporations with offices in multiple countries reported that different national operations would always need to take into account local

135 Study cybercrime questionnaire (private sector). Q24.
136 Study cybercrime questionnaire (private sector). Q26.
137 Study cybercrime questionnaire (private sector). Q24-27.
138 Study cybercrime questionnaire (private sector). Q24.
139 Study cybercrime questionnaire (private sector). Q24-27.
140 *Ibid.*
141 *Ibid.*
142 Study cybercrime questionnaire (private sector). Q30.
143 Study cybercrime questionnaire (private sector). Q35.
144 Study cybercrime questionnaire (private sector). Q28.

laws and regulations. However, multinational private sector organizations generally identified a primary 'seat' jurisdiction for the receipt of law enforcement requests globally.[145]

In addition to a general requirement for due legal process in the jurisdiction of the 'seat' of a corporation, a number of private sector organizations noted that informal foreign law enforcement requests may also be complied with on a *discretionary* basis.[146] Publically available information for global service providers such as Google, for example, states both that: '*Using Mutual Legal Assistance Treaties and other diplomatic and cooperative arrangements, [foreign] agencies can work through ['seat' national authorities] to gather evidence for legitimate investigations*', and that: '*On a voluntary basis, we may provide user data in response to valid legal process from* [*foreign*] *agencies, if those requests are consistent with international norms, ['seat' national] law, Google's polices and the law of the requesting country*.'[147]

This adds up to a picture of a default requirement for foreign law enforcement authorities to obtain requisite subpoenas, warrants or orders in the 'seat' jurisdiction of a service provider, combined with a certain discretion to supply data to law enforcement within the limits of national laws and customer terms of use. Such discretionary relationships between the private sector and law enforcement are largely built on trust and are not considered legally binding – they usually exist therefore within limited geographic or socio-political areas. One company from Central America, for example, stated that it accepted obligations derived from informal law enforcement requests, but limited compliance exclusively to those issued by local authorities.[148] One European company specified that it treated informal requests from foreign law enforcement authorities in the same way as requests by national authorities, but did not consider itself legally bound to comply in either scenario.[149] As publically noted by one leading online services provider: '*we are operating in good faith with… authorities, but we have no obligation to do so… If that good faith is abused, we would have to think much more carefully about that cooperation*.'[150] In other words, within the constraints of data protection laws and customer terms and conditions, service providers have a significant amount of latitude over data disclosed, including to foreign law enforcement agencies. These decisions are often based on existing working relationships and perceptions of trust. One global provider of network equipment, for example, stated that all requests would '*undergo review, in order to ensure technical feasibility and alignment with country-specific […] legal and […] human rights regulations*.'[151]

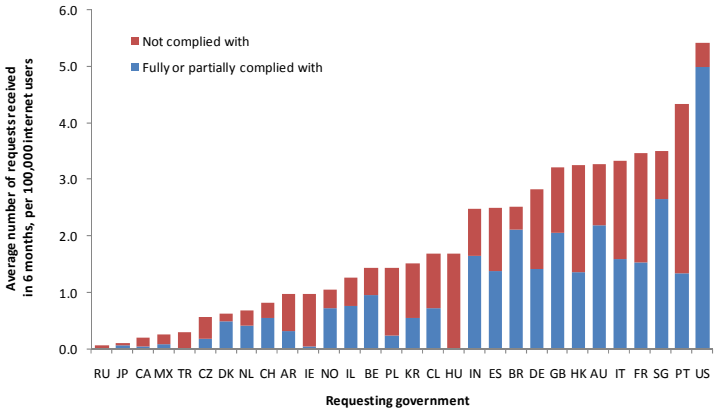
A combination of: (i) varying capacity of foreign law enforcement authorities to ensure due legal process in the 'seat' jurisdiction through mutual legal assistance; and (ii) the existence of networks of informal trust, results in variation in the extent of compliance with foreign requests for information by global service providers. Figure 5.18 shows the number of requests received and complied with from different countries (scaled per 100,000 internet users in the requesting country) as reported by Google Transparency Report.[152] The highest proportion of requests complied with are in the 'seat' jurisdiction. Requests from other countries vary from zero per cent of requests complied with, to almost 80 per cent, with an average of around 50 per cent complied with. This pattern likely derives from a number of factors, including: the extent to which foreign law enforcement requests are made informally or directly, rather than through mutual legal assistance; corporate policies towards informal requests from different countries; and the capacity of foreign authorities for the preparation of mutual legal assistance requests.

---

145 Study cybercrime interviews (private sector). Q28.
146 *Ibid.*
147 See, for example, http://www.google.com/transparencyreport/userdatarequests/legalprocess/
148 Study cybercrime questionnaire (private sector). Q28.
149 *Ibid.*
150 House of Lords and House of Commoners. *Draft Communications Data Bill Joint Committee – First Report*. Section 6 (Jurisdictional issues – Requests addressed to overseas CSPs), 28 November 2012.
151 Study cybercrime questionnaire (private sector). Q28.
152 See http://www.google.com/transparencyreport/userdatarequests/

Informal relationships between law enforcement and private sector organizations can extend more broadly than the supply of computer data for investigations. During information gathering for the Study, both countries and private sector organizations reported a wide range of areas of cooperation. One country in Northern Europe, for example, reported that '*Law enforcement has an informal working relationship with the major service providers to update contact information and to develop procedures for the formal exchange of data.*'[153] Other countries noted that '*There are voluntary codes of practice that allow sharing of information, alongside formal legislation.*'[154]

Figure 5.18: User data requests received by Google from governments (1 Jan 2011 - 30 Jun 2012)

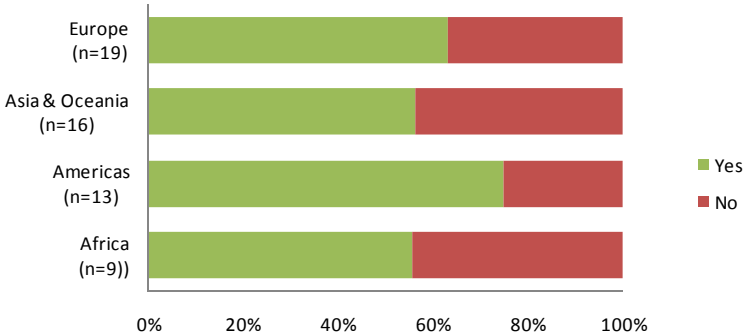


Source: UNODC presentation of Google Transparency Report data.

Several countries reported particular emphasis on relationships with telecommunications and service provider companies. One country, for instance, highlighted that: '*Agencies maintain close relationships with the telecommunications industry – particularly large industry participants. These relationships are used primarily for discussing practical measures (such as the best procedures for serving warrants, deploying capabilities and delivering lawfully intercepted information), technical issues (such as the operation of the telecommunications networks), and policy issues.*'[155] Information provided by private sector organizations also indicates that many corporations – and not just electronic service providers – engage in partnerships with law enforcement. These include for the purposes of sharing general information on cybercrime threats and trends, and with a view to facilitating reporting of suspected cybercrime cases.[156] Public-private partnerships concerning cybercrime are discussed in broader terms in Chapter Eight (Prevention).

Responses from countries to the Study questionnaire suggest that informal relationships between law enforcement and service providers are equally common across different regions. Figure 5.19 shows that between 50 per cent and 60 per cent of countries in all regions reported the existence of such relationships.[157]

Figure 5.19: Informal relationships between law enforcement and service providers



Source: Study cybercrime questionnaire. Q103. (n=56)

A number of countries were careful to point out that informal relationships between law enforcement and service providers involved information sharing '*not implicating private customer data.*'[158]

153 Study cybercrime questionnaire. Q103.
154 *Ibid.*
155 *Ibid.*
156 Study cybercrime questionnaire (private sector). Q40-45.
157 Study cybercrime questionnaire. Q103.
158 Study cybercrime questionnaire. Q103.

Others, however, seemed to indicate that individual customer data could be supplied to law enforcement authorities through such arrangements.[159] While durable and efficient relationships between law enforcement and service providers can greatly assist effective cybercrime investigations, it is critical that such arrangements also meet rule of law and international human rights standards. As discussed in this Chapter, these include sufficient clarity on the conditions and circumstances in which law enforcement authorities are empowered to obtain computer data, and adequate and effective guarantees against abuse.[160] Arrangements similar, for example, to unfettered law enforcement 'terminal' access to subscriber, traffic or content data stored by service providers may be subject to particular levels of human rights scrutiny.[161]

5.6 Law enforcement capacity

KEY RESULTS:

- Over 90 per cent of responding countries have begun to put in place specialized structures for the investigation of cybercrime and crimes involving electronic evidence
- In developing countries, however, these are not well resourced and suffer from a capacity shortage
- Countries with lower levels of development have significantly fewer specialized police, with around 0.2 per 100,000 national internet users. The rates is two to five times higher in more developed countries
- Some 70 per cent of specialized law enforcement officers in less developed countries were reported to lack computer skills and equipment

This section presents information gathered on the *capacity* of law enforcement authorities to prevent and combat cybercrime. Institutional 'capacity' in the context of policing has a number of elements, including strategic and operational capabilities, technical skills of personnel, and sufficiency of officers and resources.[162] Another important element of capacity is the degree of 'specialization.' Crimes that require a 'specialized' response are typically those that present specific challenges in terms of offence definitions, applicability of laws, or evidence gathering and analysis.[163] Cybercrime shows all of these characteristics, and a degree of law enforcement specialization is critical to an effective crime prevention and criminal justice response. Law enforcement specialization can occur at both the *organizational* and *personnel* levels – both of which often overlap. While specialization will likely always be required in the area of cybercrime and electronic evidence, it is also the case that – as the world advances towards hyperconnectivity – *all* law enforcement officers will increasingly be expected to routinely handle and collect electronic evidence.

Organizational specialization

The majority of countries that responded to the Study questionnaire reported the existence of specialized law enforcement structures for cybercrime. More than 75 per cent of countries

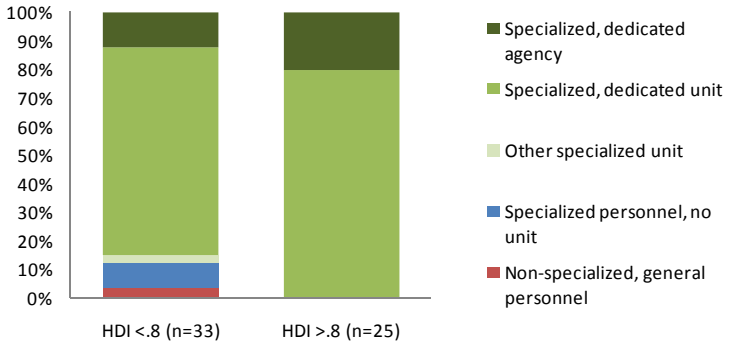
159 *Ibid.*
160 See above, Section 5.3 Privacy and investigative measures, Existence of privacy protections and procedural safeguards.
161 See, for example, http://www.edri.org/edri-gram/number6.24/bulgarian-administrative-case-data-retention
162 Katz, C.M., Maguire, E.R., Roncek, D.W., 2002. The Creation of Specialized Police Gang Units. *Policing,* 25(3):472-506.
163 Mace, R.R., 1999. *Prosecution Organizations and the Network of Computer Crime Control.* (Doctoral dissertation). AAT 9920188.

reported a specialized dedicated *unit* within existing enforcement organizations. Around 15 per cent reported a specialized dedicated *agency* for cyber or cybercrime related issues.[164]

Notably, both more highly developed countries (HDI>0.8) and less developed countries (HDI<0.8) reported significant degrees of specialization. Nonetheless, lesser developed countries showed a wider range of structures, with some countries reporting no specialized personnel, and some reporting the existence of specialized personnel, but not organized within a dedicated unit. With a single exception (in Africa), countries that reported a lack of specialized agency or unit indicated plans to establish one in the near future.[165]

Responding countries also showed variation across development levels regarding the way in which specialized units are integrated into federal, regional, state, and municipal law enforcement departments and agencies. In some countries, '*all federal investigative agencies have dedicated units on cybercrime.*'[166] Others reported federal level units with '*variable law enforcement arrangements at the State and Territory between the different jurisdictions.*'[167] There was also considerable variation reported within countries in terms of the geographic coverage and consistency of units within enforcement organizations or agencies.[168] Several countries reported the establishment of a national specialized unit or agency with additional plans to add personnel and units incrementally in field office locations.

Figure 5.20: Law enforcement structure for preventing and combatting cybercrime



Source: Study cybercrime questionnaire. Q113. (n=58)

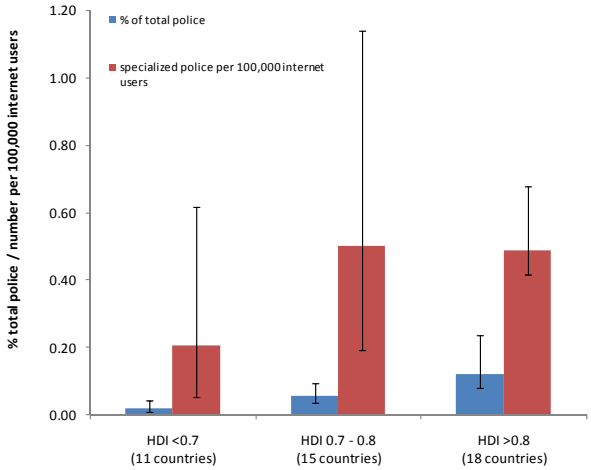
Developed countries frequently reported '*a wide range of*' or '*sufficient resources*', although several indicated that *'Resources are basically adequate to conduct investigations with a view to upgrade capabilities to a higher level*' and '*All the resources are sufficient to the point that they help us get the job done. But for improved, more efficient and faster results, we would need new and updated hardware and software resources.*'[169] Other more developed countries indicated also indicated specific personnel development needs, including '*not enough human resources* and differences between federal and state resource levels of police '*some state [level] police have adequate capabilities, some don't.*'[170] Developing countries in Africa and Asia indicated needs for '*tools for forensics*' and emphasized that '*forensic computers and computer forensic application are outdated.*'[171]

164 Study cybercrime questionnaire. Q113.
165 *Ibid.*
166 Study cybercrime questionnaire. Q113.
167 *Ibid.*
168 *Ibid.*
169 Study cybercrime questionnaire. Q109.
170 *Ibid.*
171 *Ibid.*

Personnel specialization

Many countries reported the existence of law enforcement officers specialized in cybercrime.[172] Countries with lower levels of development, however, have significantly fewer specialized police, with around 0.2 specialized officers per 100,000 national internet users. The rate is two to five times higher in more developed countries. For all countries, the proportion of police specialized in cybercrime was less than one per cent of total police.[173]

Figure 5.21: Number of specialized police, by level of country development



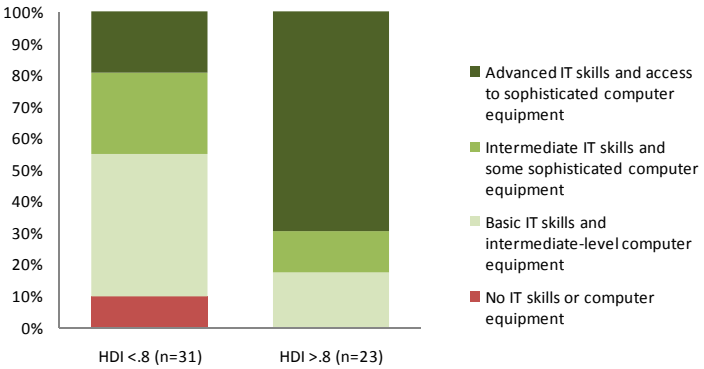
Source: Study cybercrime questionnaire. Q115 and Q61. (n=44)

Overall, around 40 per cent of responding countries reported that officers specialized in cybercrime possessed 'advanced' IT skills. Just over 30 per cent of countries reported that specialized officers reported 'intermediate' skills. Twenty per cent of countries indicated that specialized officers possessed 'basic' IT skills, and six per cent reported that specialized officers did not possess any IT skills.

This overall picture masks significant differences by country development level however. In more highly developed countries around 70 per cent of specialized officers were reported to possess advanced IT skills and to have access to sophisticated computer equipment This proportion was around 20 per cent for lesser developed countries. In contrast, in lesser developed countries, some 45 per cent of countries reported that specialized cybercrime officers possessed only basic IT skills and access to intermediate-level computer equipment.

Within a country, however, the picture may also vary significantly. One country, for example, reported that '*no general statement is possible as the whole spectrum is represented.*'[174] Some units have appropriate '*equipment and software, but the level of skill (of employees) is insufficient to address a lot of issues.*' Other units '*have advanced specialized officers, but lack sophisticated resources.*'[175]

Figure 5.22: Reported technical capabilities of law enforcement



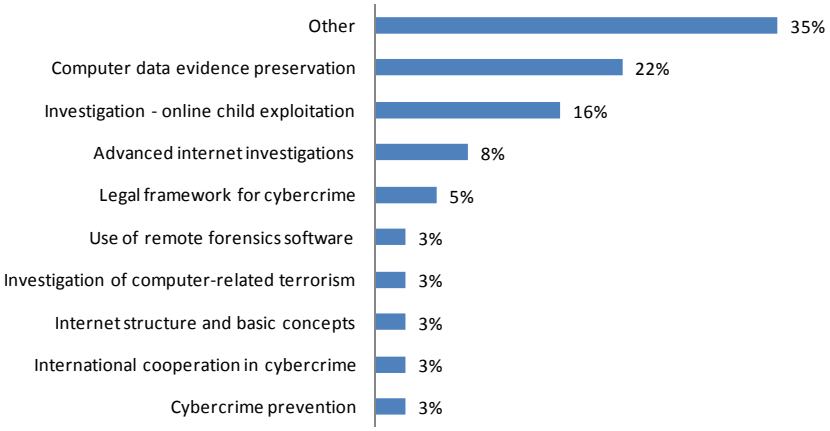
Source: Study cybercrime questionnaire. Q116. (n=54)

172 Study cybercrime questionnaire. Q115.
173 Calculations based on Study cybercrime questionnaire. Q115; and United Nations Survey of Crime Trends and Operations of Criminal Justice Systems, latest available year.
174 Study cybercrime questionnaire. Q116.
175 *Ibid.*

Personnel development

Most countries reported providing some cyber-related training to both specialized and non-specialized law enforcement personnel. Specialized law enforcement officers received training that spanned a range of topics, from technology-orientation and basic investigations, to evidence and forensics issues. Multiple training topics (35 per cent), computer evidence preservation (around 20 per cent) and online child exploitation (around 15 per cent) training were the most commonly reported subject matter for specialized officer training. Other topics included advanced internet investigations, digital forensics, use of special forensic software, and malware analysis.

Figure 5.23: Training subject matters for specialized law enforcement officers

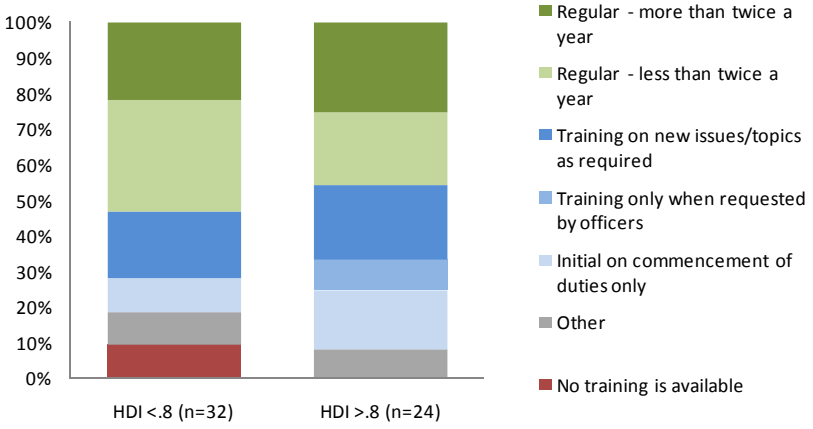


Source: Study cybercrime questionnaire. Q117. (n=37)

The extent and coverage of training programs provided to specialized officers varied widely. In some countries, all specialized officers received cybercrime training, either in person or online. In other countries, training was provided at the national level to officers in selected units on basic cybercrime terminology or basic investigative methodology. Some countries reported providing additional training on topics such as basic IT awareness, technology enabled crime awareness, data evidence preservation and remote forensics software. Training was reported as either integrated into specialized officer training or available as needed or on demand by officers.

Regular training is an important component of law enforcement capacity as it enables specialized officers to remain up-to-date with the latest techniques and developments. In both more highly developed countries and lesser developed countries, regular training (more than once a year) was reported in around 50

Figure 5.24: Frequency of training for specialized law enforcement officers

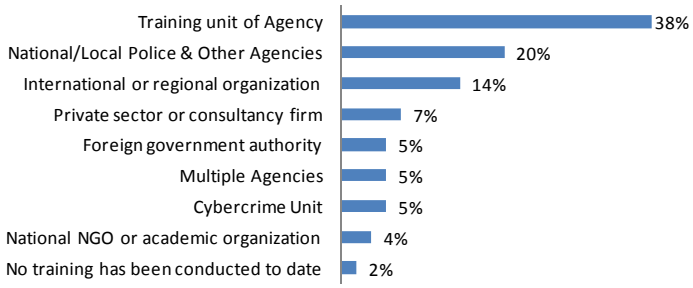


Source: Study cybercrime questionnaire. Q118. (n=56)

per cent to 60 per cent of countries. Some lesser developed countries reported, however, that training was either '*rare*' or that no training at all was available.[176]

Training for specialized officers was most often provided directly by a training unit of the law enforcement agency itself. International or regional organizations were mentioned by around 15 per cent of countries as a training provider for specialized cybercrime law enforcement officers – indicating a significant role for technical assistance delivered by these organizations. Chapter Six (Electronic evidence and criminal justice) examines needs for, and delivery of, technical assistance in greater detail.

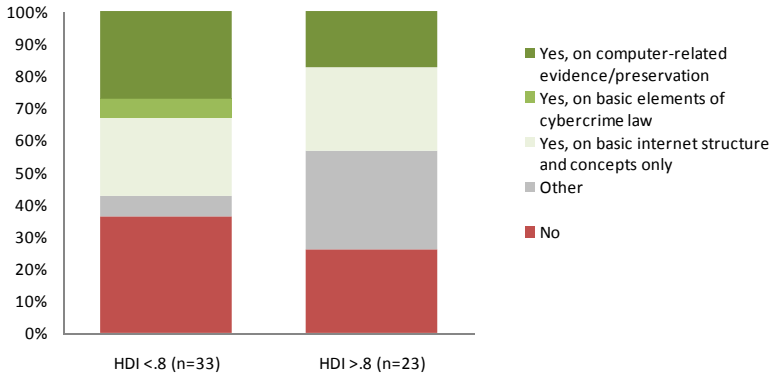
Figure 5.25: Training provider for specialized law enforcement officers



Source: Study cybercrime questionnaire. Q119. (n=56)

As electronic evidence becomes an important component in the investigation of all crime types, 'non-specialized' law enforcement officers will increasingly be required to conduct basic computer-related investigations. Responses to the Study questionnaire showed marked differences between countries concerning the delivery of cybercrime-related training to non-specialized law enforcement officers. Around 25 per cent of countries, both more highly developed and lesser developed, reported delivery of basic training on internet structure and concepts to non-specialized officers. Some 40 per cent of lesser developed countries reported, however, that non-specialized officers do not receive any training concerning cybercrime or electronic evidence. Nonetheless, a number of countries highlighted initiatives to improve cybercrime-related training for non-specialized officers. One country, for example, reported '*embarking on a 'mainstreaming' programme to give all officers a basic understanding of cyber crime and the relevant investigation techniques and legislation.*'[177] Another indicated that '*regular officers receive training on computer-related evidence preservation as part of some general investigation courses.*'[178] Others noted that cybercrime topics are '*being incorporated in the regular police education*'[179] and officer initiated training is '*available through online courses in our technology training platform.*'[180]

Figure 5.26: Training for non-specialized law enforcement personnel



Source: Study cybercrime questionnaire. Q120. (n=56)

[176] Study cybercrime questionnaire. Q118.
[177] Study cybercrime questionnaire. Q120.
[178] *Ibid.*
[179] *Ibid.*
[180] *Ibid.*

CHAPTER SIX: ELECTRONIC EVIDENCE AND CRIMINAL JUSTICE

This Chapter considers the criminal justice process in cybercrime cases, starting from the need to identify, collect and analyse electronic evidence through digital forensics. It examines the admissibility and use of electronic evidence in criminal trials, and demonstrates how a range of prosecutorial challenges can impact on criminal justice system performance. It links law enforcement and criminal justice capacity needs with a view of delivered and required technical assistance activities.

6.1 Introduction to electronic evidence and digital forensics

Key results:

- Evidence is the means by which facts relevant to the guilt or innocence of an individual at trial are established. Electronic evidence is all such material that exists in electronic, or digital form
- Digital forensics is concerned with recovering – often volatile and easily contaminated – information that may have evidential value
- Forensics techniques include the creation of 'bit-for-bit' copies of stored and deleted information, 'write-blocking' in order to ensure that original information is not changed, and cryptographic file 'hashes,' or digital signatures, that can demonstrate changes in information

Electronic evidence in criminal proceedings

Evidence is the means by which facts relevant to the guilt or innocence of an individual at trial are established. Electronic evidence is all such material that exists in electronic, or digital, form. As noted in Chapter One (Global connectivity), electronic evidence is central not only to the investigation and prosecution of forms of cybercrime, but increasingly to crime in general. Legal frameworks optimized for electronic evidence, together with law enforcement and criminal justice capacity to identify, collect and analyse electronic evidence, are thus central to an effective crime response.

During information gathering for the Study, countries were asked about the capacity of law enforcement authorities and prosecutors to collect and handle electronic evidence. Countries were also asked about legal frameworks for electronic evidence, including admissibility and evidentiary laws and rules that apply to electronic evidence. [1] Before consideration of country responses, this section contains a brief introduction to the nature of electronic evidence and the means through which it can be collected, including digital forensics.

Generating evidence – User interaction with computer devices produces a wealth of computer-generated digital traces (sometimes called digital fingerprints or artefacts). Computer data and

[1] See Study cybercrime questionnaire. Q109-112, and Q143-150.

electronic communications potentially relevant to a criminal act may include gigabytes of photographs, videos, emails, chat logs and system data. Locating relevant information within this data can be extremely time-consuming. The variety of possible file formats, operating systems, application software, and hardware particulars also serves to complicate the process of identifying relevant information.

Computer artefacts can be easily modified, overwritten or deleted, thus posing challenges where sources of digital information must be authenticated and verified.[2] Evidence rules vary considerably between jurisdictions, even amongst countries with similar legal traditions. In general terms, however, legal systems of the common law tradition tend to have defined rules as to the admissibility of evidence. In legal systems of the civil law tradition, in which professional judges retain a high degree of control over the court proceedings, admissibility of evidence may be flexible, although the weighing of evidence (including ascertaining its credibility and authenticity) can also obey a comprehensive set of rules.[3]

In many legal systems, the quality of procedures applied to maintain the integrity of digital information from the moment of creation to the point of introduction in court must be demonstrated by the proponent of the evidence. The integrity and authenticity of digital information has a direct bearing on the weight of evidence, in terms of its reliability and trustworthiness. The party seeking to introduce evidence must usually demonstrate evidence continuity, or 'chain-of-custody,' so that it can be proved that the evidence has not been tampered with or otherwise altered. Evidence continuity is typically a question of fact and the chain-of-custody process is the mechanism applied for maintaining and documenting the chronological history of the evidence as it moves from one place to another.[4]

In the case of digital information, evidence continuity must be maintained for both the *physical device* housing the data (when received or seized), and the *stored data* residing on the device.[5] As such, the party offering the evidence must demonstrate that: (i) the digital information obtained from the device is a true and accurate representation of the original data contained on the device (authenticity); and (ii) that the device and data sought to be introduced as evidence is the same as that which was originally discovered and subsequently taken into custody (integrity). The objective is to show that the device is what it is purported to be and that the digital information is trustworthy, and has not been tampered with or altered.[6]

The reliability of computer-generated and computer-stored information has also been challenged on the basis of security vulnerabilities in operating systems and programs that could give rise to threats to the integrity of the digital information. The susceptibility of digital information to manipulation has been considered by courts when introducing electronic evidence, with emphasis on '*the need to show the accuracy of the computer in the retention and retrieval of the information at issue*.'[7] The admissibility of computer-generated information (such as log file records) detailing the activities on a

---

2 See for example *United States v Whitaker*, 127 F3d 595, 602 (7th Cir. 1997).

3 See Jackson, J.D., and Summers, S.J., 2012. *The Internationalisation of Criminal Evidence: Beyond the Common Law and Civil Law Traditions*. Cambridge: Cambridge University Press.

4 Casey, E., 2011. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. New York: Elsevier.

5 U.S. Department of Justice, 2007. *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors*. National Institute of Justice, p.16.

6 Marcella Jr., A.J., Greenfield, R.S., (eds.), 2002. *Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*, 2nd edn. Boca Raton: CRC Press, p.136.

7 *Re Vee Vinhnee, Debtor American Express Travel Related Services Company, Inc v Vee Vinhnee* 336 BR 437 (9th Cir BAP, December 16, 2006), p.18.

computer, network, or other device may be open to challenge when the system generating the information does not have robust security controls.[8]

In addition to demonstrating authenticity and integrity of evidence, challenges to the use of electronic evidence arise, in some jurisdictions, from the application of particular *evidential rules*. It may need to be demonstrated, for example, that electronic evidence falls within particular exceptions to a general prohibition on 'hearsay' evidence,[9] or that a 'print-out' of computer data satisfies requirements such as a 'best evidence' rule.[10] National approaches to such issues reported through the Study questionnaire are addressed in this Chapter.

Digital forensics

Many forms of electronic evidence may be comparatively straightforward, such as a printout of a readily available email sent by a perpetrator, or IP connection logs reported directly by an internet service provider. Other forms, on the other hand, may require sophisticated techniques in order to recover traces of activity or data from computers and networks that can provide evidence of criminal behaviour. Digital forensics is the branch of forensic science concerned with the recovery and investigation of material found in digital and computer systems. To discover such traces, digital forensics experts take advantage of the tendency of computers to store, log and record details of almost every action that they, and hence their users, perform.

Forensics scenario: Evidence of computer fraud from an Internet café

Scenario: A fraud has been attempted via email. Police gain evidence that the emails in question may have been sent from a desktop computer in a local internet café

A typical internet café setup resembles, in many ways, a home network environment. It is likely to contain multiple laptop or desktop computers connecting over a combination of wireless and wired network devices. For the purposes of billing usage of computers, a cybercafé may require user identification; in several jurisdictions this is mandatory, and provides an audit trail to link an individual to a particular computer at a given time. It may also be possible to identify an individual using a computer at a given time through footage from security cameras.

If an investigation occurs swiftly enough, or if prior knowledge of activities is given, then forensic investigators may be in a position to gain physical access to the computer and to conduct a standard investigation. This process is complicated by the public nature of the device, which consequently contains traces of many users' activity.

An internet café, regularly handling more users and traffic than a home network, is likely to have additional network devices such as proxy servers that keep copies of commonly-requested web pages in order to speed up traffic; and firewall hardware for security. These devices may be analysed for traces of network activity linked to the suspicious activities of the user.

Information stored on electronic devices, including computers and mobile phones, is volatile and easily altered or corrupted in investigations. At the same time, such information is easily duplicated. A crucial first step in many digital forensics investigations is therefore to create an

8 Chaikin, D., 2006. Network investigations of cyber attacks: the limits of digital evidence. *Crime, Law and Social Change*, 46(4-5):239-256, 249.

9 Hearsay is often defined as *'evidence given of a statement made on some other occasion, when intended as evidence of the truth of what was asserted'* (*Halbury's Laws*, Vol. 17). Certain types of digital evidence may strictly constitute hearsay, but could be admitted under exceptions such as 'business records.' See Thomson, L.L., 2011. Admissibility of Electronic Documentation as Evidence in U.S. Courts. Appendix IX.B.1, Center for Research Libraries, *Human Rights Electronic Evidence Study*.

10 As a general principle, courts are entitled to the best evidence that is available. If a best evidence rule is applied, copies of an original may not be admissible as evidence unless it can be demonstrated that the original is unavailable due to destruction or other circumstances. The printout of information located on a computer or other storage device might not technically be regarded as 'original.' In some jurisdictions, however, the best evidence rule does not operate to exclude printouts, provided that the printout accurately reflects the actual data. See, for example, *Doe v United States*, 805 F. Supp. 1513, 1517 (D. Hawaii. 1992); and *Laughner v State*, 769 N.E.2d 1147, 159 (Ind. Ct. App. 2002).

undisturbed forensic *image* (or 'bit-for-bit' copy) of the storage device, containing as detailed a copy of the original device as can be obtained. By operating on the image rather than the original device, the data can be examined without disturbing the original, thus providing a safeguard against any tampering or falsification. A forensic image is typically created with the aid of a special device called a *write-blocker* that prevents any alterations being made to the original data.[11]

Forensics scenario: Evidence from a mobile carrier of conspiracy to commit a serious crime

Scenario: An individual is investigated under suspicion of conspiring to commit homicide. As part of the investigation, police request data from the individual's mobile phone network.

The capabilities of a mobile phone provider are similar to those of an internet service provider combined with a standard telephone provider, with the important addition of geolocation data that reveals a user's physical location.

Telephone traffic details, in most jurisdictions, will store dialled telephone numbers as well as the time and duration of the call. Wiretap capabilities function much as those of other telephony providers. This information can reveal patterns of calls to other individuals, as well as providing correlations between real-world events, such as a phone call made shortly after a crime was committed.

The most significant difference with mobile phones, however, is that the device is typically carried by the owner at all times, and constantly connects to local mobile base stations that relay the phone's signals. By tracking the base stations to which a phone connected at a given time, the location of the owner can be inferred within a given region. If actively triangulated using multiple base stations, a phone can be localized to within tens of metres.

Depending on jurisdiction and data retention policies, providers may store the geographical location of mobile phones whenever they send or receive messages or phone calls, as in the case of the European Union's Data Retention Directive. Others jurisdictions may not store this data at all, except when explicitly requested by law enforcement, at which point explicit triangulation of location may allow for accurate location of an individual via their phone.

In addition to the ability to create a 'bit-for-bit' copy of stored information, other important forensics tools include the use of 'data carving' or 'file carving' that can retrieve deleted or corrupted files from the remnants of raw data that remain on storage devices even after the original file is gone.[12] In addition, to compare files quickly and accurately, analysis tools make use of cryptographic *hashes* that correspond to a small and unique 'signature' for a given piece of data. Changing the data by even the slightest amount results in a different hash.

Different devices require different investigative and forensic techniques. Examination of mobile devices requires a different set of tools to those employed when examining a desktop computer or network server. Varying types of hardware, software and operating systems each present their own challenges associated with retrieving information.

Computer forensics focuses on analysing traditional desktop computers and laptops as found in both homes and businesses. Computers usually contain high-capacity hard drives that store a great deal of information, including photos and videos, as well as histories of web browsing, and email and instant messaging information. They typically run a small number of well-known operating systems including Windows, Mac OS, and Linux.

Mobile device forensics examines low-powered mobile devices, with smaller capacity for storage compared to computers, and with simpler software to facilitate phone calls and internet browsing. The gap between phones and computers is, however, getting smaller in terms of functionality,

11 US National Institute of Standards and Technology, 2004. *Hardware Write Blocker Device (HWB) Specification, Version 2.0*.

12 Gutmann, P., 1996. Secure Deletion of Data from Magnetic and Solid-State Memory. *Proceedings of the 6th USENIX Security Symposium*.

processing power and software. A distinguishing feature of mobile phones is their mobility – they are usually with their owner at all times – and their constant connectivity. This extends to monitoring reasonably accurate geographic location in modern systems. Mobile phones often contain both a relatively complete contact list, as well as call records. All data and information typically flows over the mobile ISP's network, enabling investigators to obtain a large range of information related to the use of the phone. Tablet devices are often simply scaled-up versions of a mobile phone, making tools designed for mobile phones also applicable.

Case example: Identifying an internet extortionist (A country in North America)

One law enforcement investigation into an alleged extortionist demonstrates some of the techniques used to track down online criminals. The accused threatened to post sexual images of his victims on their own social networking pages.

Investigators received information from the security division of the social networking site about logins to the victims' accounts, all originating from a single IP address. Someone at that IP address had accessed 176 different accounts in less than two months, mostly from the same computer. Many of the users of those accounts had disabled their accounts after being hacked. The same IP address had been used to access the suspect's own account 190 times, more than any other address. It had also been used to login 52 times to one of the victims' webmail accounts. A separate login to the suspect's account occurred from an IP address registered to a company listed as the suspect's employer on his social network profile. On this basis, a request was made to an ISP for subscriber information connected to the IP address. Within one week, the ISP responsible for the suspect's IP address provided subscriber information, including a physical address that matched other public records. Investigators executed a search warrant at this premises, seizing further evidence used to indict the suspect later the same month.

Source: http://www.justice.gov/usao/cac/Pressroom/2013/016.html and http://arstechnica.com

Network forensic techniques are critical now that mobile phones and computers, and many of the actions for which they are used, are associated with online services and cloud storage. These services store data on the internet rather than the user's device, reducing the amount of information that can be gathered without the use of network analysis. Network traffic is largely transient. In order to gain detailed information about activities taking place on a network, traffic must be actively gathered and stored for subsequent analysis. This can include analysis of log files from network devices such as firewalls and intrusion detection and prevention systems, as well as analysing the content of logged network traffic, if available.[13]

In situations where an attacker may have gained electronic access to a computer system, any data on that computer may have been compromised by the attacker. In such cases, log files of that system's activity are likely to be considered unreliable, and network forensics may be the only form of data available to an analyst. The major challenge in a forensic investigation of a network lies in reconstructing the actions that have taken place across a network from the limited log data available. This may be used to identify hacking attempts, unauthorized access to systems and denial of service attempts, as well as data concerning which resources were accessed by individuals at given times.

[13] Chappell, L., 2012. *Wireshark Network Analysis (Second Edition): The Official Wireshark Certified Network Analyst Study Guide*. Laura Chappell University.

6.2 Capacity for digital forensics and electronic evidence handling

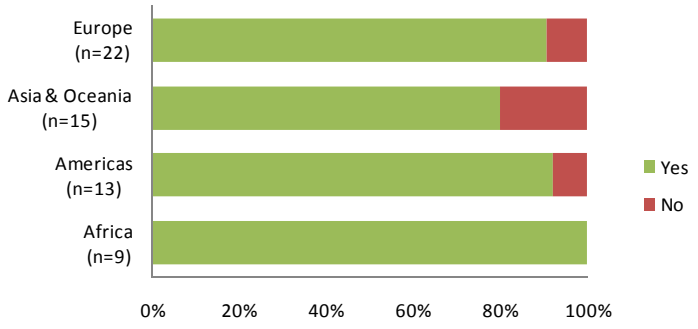
Key results:

- While almost all countries have some digital forensics capacity, many responding countries, across all regions, report insufficient numbers of forensic examiners, differences between capacity at federal and local level, lack of forensics tools, and backlogs due to large quantities of data for analysis
- Over half of countries report that suspects make use of encryption, rendering access to this type of evidence difficult and time-consuming without the decryption key
- All countries in Africa and one-third of countries in other regions report insufficient resources for prosecutors to handle and analyse electronic evidence
- Electronic evidence is admissible in court in more than 85 per cent of responding countries, although in small number legal obstacles such as the inadmissibility of all electronic evidence, and the inadmissibility of extraterritorial electronic evidence, present serious obstacles to the prosecution of cybercrime acts

Forensics capacity

The ability of law enforcement to collect and analyse electronic evidence during investigations can be critical to the successful identification and prosecution of perpetrators. Responding countries to the Study questionnaire indicated a range of capacities in this regard. More than 90 per cent of countries, across all regions of the world, reported some capability to conduct digital forensics-based investigations.[14] Additional information provided by countries on access to forensic resources and levels of capability, however, reveals a more divergent picture. Less than half of countries in Africa and around two-thirds of countries in the Americas reported sufficient law enforcement resources (such as electricity, hardware, software, and internet access) for carrying out investigations and analysing electronic evidence.[15] In contrast, almost 80 per cent of countries in Europe, and Asia and Oceania, reported sufficient resources.

Figure 6.1: Law enforcement capabilities to conduct electronic forensics



Source: Study cybercrime questionnaire. Q110. (n=59)

However, many countries including some developed countries, reported challenges associated with processing large volumes of data and an increasing number of devices submitted for forensic analysis.[16] One country in Europe, for example, reported that '*On a national level the police are capable of performing high level computer forensics. At a district and local level there is only capacity to undertake basic computer forensic work.*' The same country noted that '*The increasing amount of electronic evidence seized during the investigation of all kinds of crimes is a challenge, especially to the local*

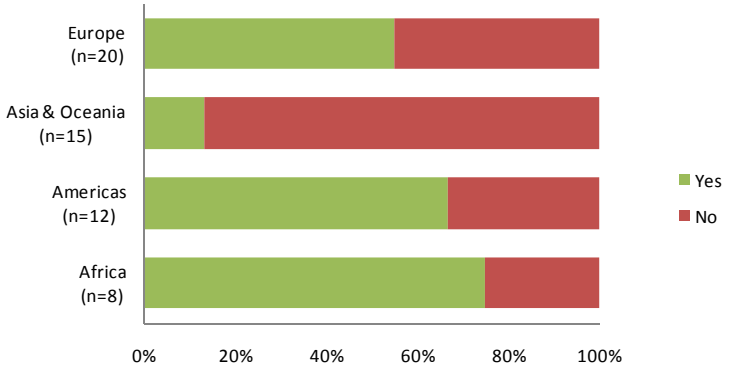
[14] Study cybercrime questionnaire. Q110.
[15] Study cybercrime questionnaire. Q109.
[16] Study cybercrime questionnaire. Q110.

police who handle a large amount of cases.' Similarly, one country in the Americas highlighted that '*The challenge is not in the expertise, but in the quantity of data that must be analysed*,'[17] and another noted that '*the amount of seized information and data is causing more and more problems for storing and analysis.*'[18]

While some countries reported a federal or centralized capacity of a '*central [forensics] laboratory and peripherals that are in charge of expert analysis of electronic evidence seized in police investigations*'[19] others reported using a distributed approach with '*forensic units throughout the country*'[20] that '*conduct electronic forensic examinations with specialized forensic tools…used on networks, computer systems, cellular phones, and storage devices.*'[21] Many countries, especially developing countries, highlighted a lack of resources for technical forensics equipment and challenges in recruiting personnel with sufficient skills to conduct investigations and process electronic evidence. One country in Africa, for example, stated that '*A few forensic examiners are available at the Federal level, but not enough to serve the whole country. Only one laboratory is functional.*'[22]

A number of countries reported encountering encryption of data during the course of law enforcement investigations and analysis of electronic evidence. Between around 60 and 80 per cent of countries in all regions, with the exception of Asia and Oceania, reported that electronic evidence was often encrypted by suspects.[23] Several countries reported an increase in use of encryption by perpetrators. One country observed that '*depending on the crime type, encryption is becoming much more common.*'[24] This view was not universal however. One country from Europe, for example, reported that '*collected evidence is very rarely encrypted compared to the enormous amount of seized data.*'[25] In addition, it is unclear whether the low proportion of encryption reported by countries in Asia and Oceania is due to differences in underlying use of encryption by suspects, or to capacities of law enforcement to detect and analyse encrypted material.

Figure 6:2: Electronic evidence encrypted by suspects



Source: Cybercrime study questionnaire. Q112. (n=55)

Countries noted that there was '*no simple way*' to overcome the '*daunting challenge*' of encryption *'that requires expert technical assistance and capacity.*'[26] Several countries indicated that they did not possess the means or tools to address the problem of encryption, without obtaining or seizing keys from the suspect. One country reported, for example, that: '*If the suspected is arrested or known, then the decryption keys are obtained from the suspect during investigation.*'[27] Some jurisdictions have legal remedies to compel cooperation.[28] If the suspect will not reveal decryption keys, investigators may use a

17 Study cybercrime questionnaire. Q109.
18 *Ibid.*
19 *Ibid.*
20 *Ibid.*
21 *Ibid.*
22 Study cybercrime questionnaire. Q111.
23 Study cybercrime questionnaire. Q112.
24 *Ibid.*
25 *Ibid.*
26 *Ibid.*
27 *Ibid.*
28 The *Regulation of Investigatory Powers Act 2000* in one country in Northern Europe, for example, provides the power to impose a disclosure requirement upon a suspect to divulge the key to protected information in their possession. Failure to comply with a

variety of software programs, engage technical expertise, or refer the potential evidence to their forensics labs or specialized personnel for attempted decryption. One country mentioned using '*certified professionals and certified software*'[29] in decryption efforts. Other countries referred to the possibility of arresting a suspect '*while the machines are open, up, and running*'[30] when data may be in an unencrypted state.

In addition to the challenges presented to digital forensics by encryption technology, perpetrators may also make use of 'steganography' (information 'hiding'). This involves concealing information or communications within otherwise innocent files, such as graphic images, documents, audio samples or applications. Media files are ideal hosts for steganography as they are typically large and will not immediately arouse suspicion. From a forensic perspective, identification of hidden data may be achieved by comparing suspect files or data streams with known originals. A number of responding countries highlighted a general increase in use of obfuscation techniques and encryption. One country in the Americas reported '*criminal organizations try to make investigations difficult by storing criminal data in foreign servers or in cloud storage systems, and use cryptography and other data obfuscation techniques.*'[31]

Increasing use of cloud computing presents particular challenges for digital forensics. Information stored remotely by perpetrators in cloud services may become visible to investigators during a search or forensic examination – such as when live internet sessions are encountered on running computers, or through remote services available on seized mobile devices. In addition to legal considerations associated with direct law enforcement access to extraterritorial data (examined in Chapter Seven (International cooperation)), cloud data storage complicates the forensic process of identification, collection, and analysis of electronically stored information.[32] The possibility that one cloud user may gain access to another's data also introduces the possibility of further challenges to data authenticity.

Faced with such challenges, responding countries reported that a variety of techniques are used to ensure that the integrity of electronic evidence collected through digital forensics is maintained. Countries referred, for example, to the use of forensic imaging; the use of sworn statements attesting to the authenticity of data; forensic hash values; the use of write blockers; capture of internet data through screen shots; systematic labelling, documentation, packaging and transportation methods; and sealing of forensic images recorded on optical disk.[33] With respect to standards and guidelines for forensic investigations, a few countries referred to the Association of Chief Police Officers' Good Practice Guide for Computer-Based Electronic Evidence.[34]

Countries also reported a number of practices for storing electronic evidence in order to protect against degradation and damage. These included the use of multiple clone copies from a single master copy; storage of computer data within a designated IT-forensic network under restricted access; the use of humidity, temperature, and electromagnetic radiation controlled

---

notice to disclose can result in a term of imprisonment and/or fine upon conviction. Similarly, the *Cybercrime Act 2001* in one country in Oceania allows a magistrate to make an order requiring a specified person to provide any information or assistance that is reasonable and necessary to allow a law enforcement officer to access data held in or accessible from a computer.

29 *Ibid.*

30 *Ibid.*

31 Study cybercrime questionnaire. Q85.

32 Reilly, D., Wren, C., and Berry, T., 2011. Cloud computing: Pros and Cons for Computer Forensic Investigators. *International Journal Multimedia and Image Processing*, 1(1):26-34, 33.

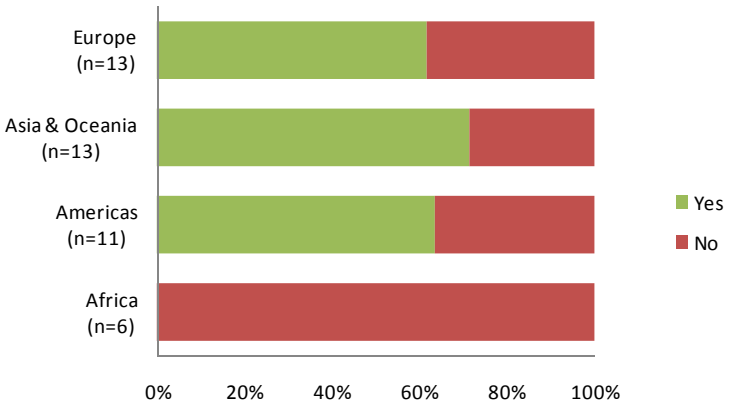
33 Study cybercrime questionnaire. Q111.

34 See http://www.met.police.uk/pceu/documents/ACPOguidelinescomputerevidence.pdf

facilities; the use of safes; the use of anti-static devices; use of supervised evidence lockers; and use of sealed bags.[35]

In addition to law enforcement capacity for digital forensics, it is also important that *prosecutors* have sufficient resources to handle and analyse electronic evidence. Electronic evidence that is not presented at trial can play no role in helping just adjudication of the accused. Country responses show that prosecutors typically report a lower level of resources for handling electronic evidence than for law enforcement.[36] Some countries, for example, commented that prosecutors often experience difficulty in making sense of electronic evidence and require the assistance of other professionals to identify trends and give data meaning.[37] None of the African respondents reported that prosecutor resources for electronic evidence were sufficient – highlighting an urgent area for focus in technical assistance and support.

Figure 6.3: Sufficiency of resources to handle and analyse electronic evidence

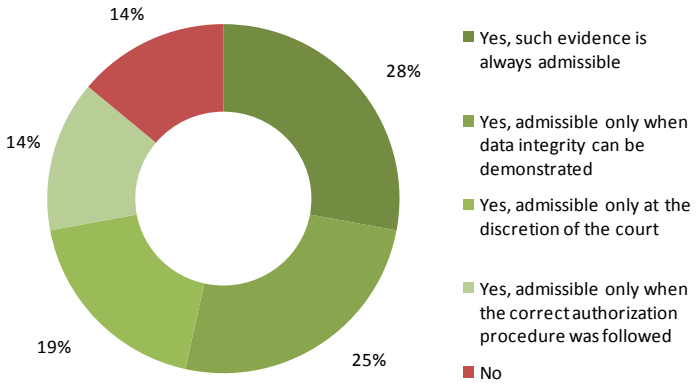


Source: Study cybercrime questionnaire. Q149. (n=44)

Electronic evidence in criminal proceedings

More than 85 per cent of responding countries reported that electronic evidence was admissible in criminal proceedings.[38] A small number of countries – predominantly in Africa and Asia – stated, however, that electronic evidence was not admissible. One country in Africa, for example, held that electronic evidence was '*Not defined in our law and hence inadmissible.*'[39] Where this is the case, a serious obstacle to the successful prosecution of cybercrime and crimes involving electronic evidence exists. For those countries where electronic evidence is generally admissible in criminal proceedings, such admissibility is subject to conditions, such as the

Figure 6.4: Electronic evidence admissible in criminal proceedings

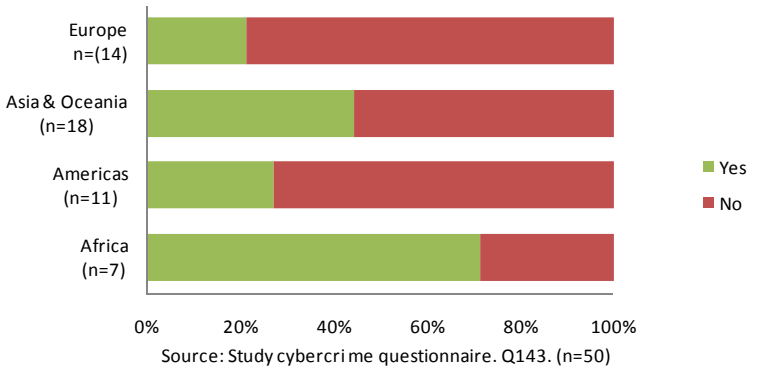


Source: Study cybercrime questionnaire. Q144. (n=43)

35 Study cybercrime questionnaire. Q111.
36 Study cybercrime questionnaire. Q149.
37 Study cybercrime questionnaire. Q149.
38 Study cybercrime questionnaire. Q144.
39 Study cybercrime questionnaire. Q143.

demonstrated integrity of the data, the discretion of the court, or authorization procedures, in around 70 per cent of countries.[40]

Figure 6.5: Legal distinction between electronic evidence and physical evidence



Source: Study cybercri me questionnaire. Q143. (n=50)

Despite general recognition of electronic evidence in national courts, one country reported not recognizing electronic evidence from *outside* of its jurisdiction.[41] In the case of a transnational crime such as cybercrime, such a restriction can impact upon the possibility for successful prosecutions. A number of countries reported that admissibility issues for extraterritorial electronic evidence often turn on whether mutual legal assistance procedures have been properly followed. One country, for example, emphasized that '*foreign evidence adduced in criminal proceedings must be in the form of testimony and any exhibit annexed to such a testimony…; testimony must be taken under oath or affirmation, under such caution or admonition as would be accepted by the court in the foreign country, or under an obligation to tell the truth imposed, whether expressly or by implication, by or under a law of the foreign country, and the testimony must purport to be signed or certified by a judge, magistrate or officer.*'[42] In many jurisdictions, such requirements frequently prevent extraterritorial electronic evidence obtained through *informal* police-to-police channels from being relied upon in criminal trials.

The greater number of countries that admit electronic evidence reported that it is treated in the same way as physical evidence. Just under 40 per cent of countries, for example, reported the existence of a legal distinction between electronic and physical evidence.[43] While approaches vary, many countries considered that it was good practice not to make a distinction, as this ensures fair admissibility of electronic evidence alongside all other types of evidence. For countries without a legal distinction between electronic and physical evidence, many reported that electronic evidence, like its traditional counterpart, '*must be: admissible; authentic; accurate; complete and convincing to juries.*'[44] Admissibility of electronic evidence was also reported to be dependent on the general rules that apply to all evidence, including that the elements '*were obtained legally, respecting the principles of relevance and abundance.*'[45] In a few countries, courts have the discretion to '*to decide whether any* [*electronic*] *evidence is admissible or not.*'[46]

Electronic evidence was reported to be transferred to prosecution or judicial authorities, and used in a criminal trial, in a number of ways. Responding countries reported all of: the physical transportation of seized computers to court; the use in court of copies of computer data stored on optical disk; the use in court of printouts of electronic evidence filed in binders; and the presentation of an expert analytical report and testimony only to the court (with the computer data remaining in storage).[47] A few countries stated, for instance, that electronic documents or data '*must be printed out*

40 *Ibid.*
41 Study cybercrime questionnaire. Q145.
42 *Ibid.*
43 Study cybercrime questionnaire. Q143.
44 Study cybercrime questionnaire. Q143.
45 Study cybercrime questionnaire. Q144.
46 *Ibid.*
47 *Ibid.*

before it is possible to read it out in the main hearing.'[48] Some countries also emphasized that '*only the relevant part of the collected evidence is transferred to prosecutors – irrelevant material or data is stored with the police.*'[49]

Countries also provided details on a number of forms and means by which electronic evidence might be presented in court. These included through testimony delivered by police officers; through testimony delivered by forensic practitioners, including presentation of digital information on projectors and widescreen monitors; and through printouts identifying objects, documents, photographs, logs, and screen captures.[50] One country in Asia focused on the use of expert reports, noting that '*Usually written reports are presented with explanations concerning the technical data.*' Other countries recounted the presentation of electronic evidence on computer screens: '*In a sophisticated computer crime case, the user of a projector in court, as a way of screening the evidence, has provide itself as an efficient way to pass the information from the prosecution to the court.*'[51]

Still others reported multiple means of presentation. One country in Europe, for example, noted that presentation of electronic evidence in court '*Depends on the actual state and place of the evidence.* [*electronic evidence may be introduced as*] *hardcopy prints, digital media (hard drives, CD, DVD, flash drives), laptop or desktop presentations, remote presentations and [live] access in rare cases.*' Some countries, however, highlighted that courtrooms were not typically set up for the use of technology in criminal trials. One country in the Americas, for instance, reported that '*Electronic trials are not yet common place. Not all courtrooms are wired for the purpose of allowing the [State] to present its case electronically. Currently the [State] must obtain the consent of the judge and defence counsel to use technology in the courtroom.*'[52]

Very few countries reported the existence of special evidentiary laws governing electronic evidence. For those that did, laws concerned areas such as legal assumptions concerning ownership or authorship of electronic data and documents, as well as circumstances in which electronic evidence may be considered authentic.[53] Other countries provided information on the way in which 'traditional' rules of evidence may be interpreted in the context of electronic evidence. One country from Oceania, for example, clarified how the 'hearsay' rule applied to electronic evidence in its jurisdiction: '*For electronic evidence specifically, the hearsay rule would not apply if the information contained in the electronic evidence relates to a communication which was transmitted between computers and has been admitted in order to identify the sender, receiver, date and time of the transmission.*'[54] Another country also noted that a '*general presumption*' exists that '*where evidence that has been produced by a machine or other device is tendered, if the device is one that, if properly used, ordinarily produces that outcome, it is taken that the device was working properly when it produced the evidence.*'[55]

Finally, countries reported on the *ways* in which electronic evidence could be used to establish a link between a criminal act and a specific perpetrator. The nature of cybercrime means that a *mediating* device, in the form of a computer system, is usually situated between the perpetrator and the victim – leading to challenges in *attribution* of acts to specific persons. In cases where a defendant is prosecuted, for example, for possession of illegal computer content, it must be established that the content was knowingly placed on the device by the defendant, and not by another person with access to the device. In this respect, one country commented that: '*Circumstantial evidence will often be the only means by which to establish identification of who is speaking or*

48 *Ibid.*
49 Study cybercrime questionnaire. Q143.
50 Study cybercrime questionnaire. Q150.
51 *Ibid.*
52 *Ibid.*
53 Study cybercrime questionnaire. Q147.
54 Study cybercrime questionnaire. Q146.
55 Study cybercrime questionnaire. Q143.

communicating. The following methods have proven helpful: proving possession of the communication device (seizure upon arrest or execution of a warrant), subscriber information, surveillance (pursuant to a court authorization, where required), analysis of the content of the communication, and forensic examination of the communication device.'[56] Another country observed that *'there are often multiple different sets of electronic evidence that must be brought together to place a suspect behind an electronic device at a particular time and place.*'[57]

Most countries reported that specific steps or criteria to establish this link did not exist. Rather, countries referred to a variety of traditional and cyber-specific techniques to '*associate the electronic evidence to a computer system under the control of [the] defendant, or to which [the] defendant has access. Standard proof techniques apply including motivation, opportunity, corroborative non-electronic evidence, control of evidence, state-of-mind evidence, and evidence which supports excluding others.*'[58]

Overall, responding countries reported a significant amount of accumulated knowledge in the area of identification, collection, analysis, and presentation of electronic evidence. Good practices in this area were highlighted not only by developed countries, but also by a number of developing countries – indicating increasing levels of global dialogue and dissemination of technical standards in the areas of electronic evidence. Nonetheless, many institutions in developing countries – including law enforcement and prosecution authorities – highlight a significant lack of capacity and resources to fully implement such standards. In addition, in a few countries, legal obstacles such as the inadmissibility of all electronic evidence, and the inadmissibility of extraterritorial electronic evidence, present serious obstacles to the prosecution of cybercrime acts.

6.3 Cybercrime and the criminal justice system in practice

Key Results:

- Prosecutors report a range of challenges to the successful prosecution of cybercrime, including sufficiency of legal frameworks, difficulties in the attribution of acts to individuals, delays due to international cooperation procedures, and evidentiary challenges
- Such challenges are reflected in available statistics on the ratio of suspects to police-recorded acts, and in 'attrition' measures that compare the number of convictions with the number of recorded acts

This section widens the discussion from forensics and electronic evidence to the performance of the criminal justice system, as a whole, in cybercrime cases. It considers challenges and good practices reported by prosecutors and courts, and identifies the possible impact of these on prosecutions and convictions of cybercrime perpetrators.

Prosecution challenges and good practices

Responding countries identified prosecution good practices and challenges across the criminal justice process, from case intake to final case disposition. Once country, for example, proposed a comprehensive set of good practices in the areas of case management, evidence disclosure, and presentation of evidence at trial: '*1) Collaborate/communicate early on with investigators, IT*

[56] Study cybercrime questionnaire. Q148.
[57] *Ibid.*
[58] *Ibid.*

personnel, paralegals and defence counsel. 2) Address quality control safeguards, e.g., business rules. 3) Inventory investigation and index disclosure. 4) Identify an expert witness who can testify to quality control issues such as completeness and integrity of prosecution database. 5) Ensure compatibility/interoperability of police/government computer systems. 6) Meet and confer with defence counsel early in the case. 7) Avoid mixing media. 8) Be able to defend the disclosure. 9) Think about metadata from the beginning and seek assistance/support from experts. 10) Ensure e-documents have been properly redacted. 11) Pick the right e-tool to fit the type of evidence you will present at trial. One size does not fit all. 12) Get the judge's permission. 13) Identify trial exhibits early, test the equipment in office/courtroom, have a backup plan, and be prepared.'[59]

Reported obstacles to successful prosecution generally related to the sufficiency of the legal framework, identification of suspects, availability and interpretation of evidence, and the proper evidence handling procedures.

With respect to legislation for procedural powers (discussed in Chapter Five (Law enforcement and investigations)), responding countries highlighted, for example, that '*lack of a legal framework*', '*lack of procedural legislation*', '*lack of proper investigatory powers which do not compromise the right to privacy and free speech in an excessive way,*' and lack of '*specific legislation on privacy protection*'[60] complicates and delays investigations.

Prosecutors also identified the challenge discussed in the previous section of this Chapter of attribution of evidence of an act to an individual. One country, for example, stated that '*In general, attribution is the hardest thing in a cybercrime investigation, so therein lies a practical obstacle to successful prosecution.*'[61] Prosecutors from responding countries further highlighted the challenges of cases with an extraterritorial dimension, including '*difficulty in obtaining evidence requiring international cooperation of other countries,*' and '*delay in the investigation and prosecution of cybercrime offences*' due to formal international cooperation processes, such as mutual legal assistance.[62]

Evidentiary issues were reported as major barriers to successful prosecution, including '*the large volume of evidence*', '*the short period of time during which service providers store information needed for investigation purposes*' and '*maintaining integrity of electronic evidence from the time of seizure to the point of completion of the case*', '*failure to establish chain of custody of evidence, and lack of proper storage facilities to maintain evidence.*'[63] '*The production of cybercrime evidence is still a challenge in court*' and '*lack of integrity of evidence from improper handling thereof by law enforcement*'[64] were also identified as particularly challenging by several countries.

Countries repeatedly reinforced the importance of evidence collection and presentation. '*Close working relationships on the prosecution team between the prosecutor and investigator that result in collection of all relevant properly authenticated evidence*'[65] are essential to success in prosecution. '*Hardware, and where appropriate software, are to be seized from the accused as quickly as is lawfully possible… followed by rapid evaluation by specially-trained highly skilled staff or external specialists.*'[66] '*Separate identification and tracking of all the relevant computer documents/images,*'[67] a '*clear chain of custody of exhibits,*'[68] and '*developing policies in*

59 Study cybercrime questionnaire. Q142.
60 *Ibid.*
61 *Ibid.*
62 *Ibid.*
63 *Ibid.*
64 *Ibid.*
65 Study cybercrime questionnaire. Q142.
66 Study cybercrime questionnaire. Q183.
67 Study cybercrime questionnaire. Q142.
68 *Ibid.*

relationship to evidence presentation in court based on successful previous presentations'[69] were important components of successful prosecutions and convictions. Finally, a '*perceived lack of fluency in the legal community with respect to technological concepts and how these impact the administration of justice*'[70] and '*understanding of digital evidence by judicial officers*'[71] were reported as additional obstacles to successful prosecution and conviction in cybercrime cases.

Additional training and resources were indicated as challenges, including '*better guidance to the courts at all levels by summarizing (and sharing) judicial experience to allow identification and uniform standards in computer information system security cases.*'[72] One country highlighted that '*It is important and decisive for good management of cybercrime cases, that the national courts have adequate financial means to acquire necessary technical equipment.*'[73] The necessity for public-private partnerships with '*internet access providers, website hosting providers, and other service providers*'[74] and banking and telecommunications companies was also reported as a productive method to enhance evidence collection.

Criminal justice system effectiveness and outcomes

Core aims of the criminal justice response, to any crime, are to achieve just outcomes for perpetrators and victims, alongside specific deterrence, rehabilitation and societal reintegration for convicted offenders, and a sense of general deterrence for potential perpetrators.[75] Measurement of how 'efficiently' or 'effectively' this is achieved is extremely challenging. Measures range from 'attrition' rates that provide information on the numbers of persons suspected, prosecuted, and convicted by the criminal justice system for specific crimes, to measures of 'timeliness' of case disposition, 'punitivity' and 'recidivism.'[76] While such measures are commonly reported, it should be noted that they do not represent direct indicators of the 'quality' of justice, and can be heavily influenced by differences in criminal justice system mechanisms, such as the application of suspect counting rules, thresholds applied in recording of cases, or prosecutorial involvement in the initial investigation stage.

Nonetheless, with a view to further understanding the criminal justice system response to cybercrime, the Study questionnaire asked countries to report available statistics on the number of recorded cybercrime offences, and numbers of persons suspected (or 'brought into formal contact with the police') for cybercrime offences, as well as numbers of persons prosecuted and convicted for cybercrime offences.[77]

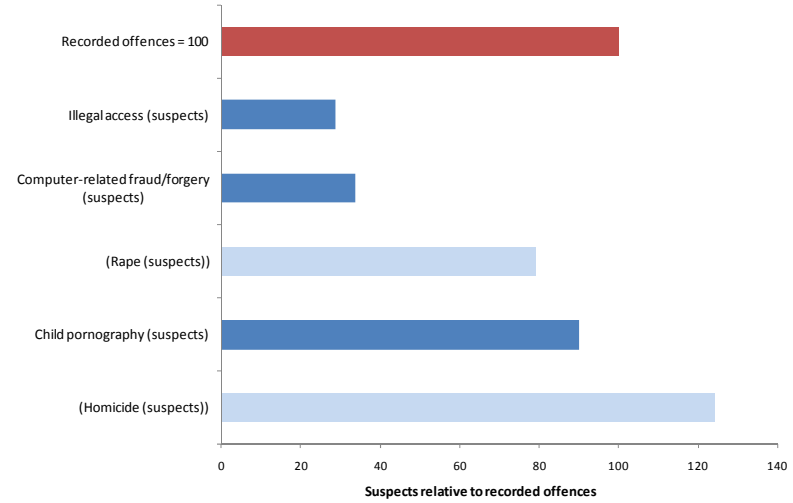
As noted in Chapter Two (The global picture), reported police statistics were found not to represent a strong basis for cross-national comparative measurement of cybercrime trends.[78] Law enforcement and criminal justice statistics *within* individual countries may, however, allow case and suspect 'attrition' calculations for that country, where reported case numbers are not small, and year-to-year effects (such as cases carried over from one year to the next) can be accounted for.

---

69 *Ibid.*
70 Study cybercrime questionnaire. Q141.
71 *Ibid.*
72 Study cybercrime questionnaire. Q142.
73 Study cybercrime questionnaire. Q183.
74 *Ibid.*
75 Albanese, J.S., 2012. *Criminal Justice.* 5th edn. Upper Saddle River: Prentice Hall.
76 See for example, Harrendorf, S., Smit, P., 2010. Attributes of criminal justice systems – resources, performance and punitivity. *In*: European Institute for Crime Prevention and Control Affiliated with the United Nations (HEUNI). 2010. *International Statistics on Crime and Justice.* Helsinki.
77 Study cybercrime questionnaire. Q54-70, Q121-137, and Q165-181.
78 See Chapter Two (The global picture), Section 2.1 Measuring cybercrime, and Section 2.3 Cybercrime perpetrators, 'Typical offender' profiles.

In general, responding countries were able to provide comparatively few law enforcement, criminal justice, and court statistics. For a set of six countries, mostly in Europe, however, it was possible to calculate the average number of persons brought into formal contact with law enforcement authorities per recorded offence for the cybercrime acts of illegal access, computer-related fraud and forgery, and child pornography offences.

Figure 6.6: Persons brought into formal contact per recorded offence (6 countries)

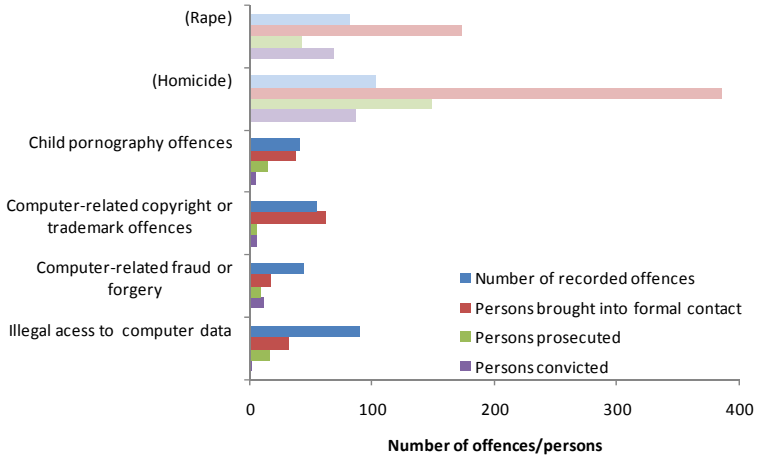


Source: Study cybercrime questionnaire. Q54-70.

Figure 6.6 shows these results alongside the suspects to offence ratios for rape and homicide in the same six countries.[79] A significant difference exists between child pornography offences and the other computer offences of illegal access and fraud or forgery. Suspect to offence ratios for child pornography are similar to that for 'conventional' crimes. Those for illegal access and computer-related fraud or forgery are significantly lower – representing around 25 recorded suspects per 100 offences.

This may be indicative of a number of factors, including differences in police investigative capabilities for different cybercrime offences, differences in police investigative focus, and variations in the point at which different cybercrime acts are recorded as offences for statistical purposes. In addition, however, the pattern may reveal genuine underlying differences in the steps taken by, and capabilities of, perpetrators to conceal criminal activity and to evade detection by law enforcement investigations.

Figure 6.7: Criminal justice system attrition in cybercrime cases



Source: Cybercrime study questionnaire. Q54-70.

While suspect to offence ratios could be calculated as an average for a number of countries, sufficient statistics for calculation of a complete 'offence to conviction' attrition rate were provided by only one country in response to the Study questionnaire. Figure 6.7 shows the number of police recorded offences,

[79] Study cybercrime questionnaire. Q54-70; and United Nations Survey of Crime Trends and Operations of Criminal Justice Systems, latest available year.

persons brought into formal contact, persons prosecuted and persons convicted for four cybercrime acts in one country in Eastern Europe, alongside equivalent data for the 'conventional' crimes of rape and homicide. The data confirm the picture of a higher number of suspects per recorded offence for child pornography offences than other cybercrime acts. This pattern is repeated for another content-related offence – that of computer-related copyright or trademark offences. In general, however, all cybercrime offences show far fewer persons prosecuted or convicted than for the conventional crimes. For the reporting country, cybercrime convictions represent, on average, 10 per cent of police-recorded offences, compared to around 80 per cent for rape and homicide.

The pattern demonstrates that the large number of cybercrime prosecution challenges referred to by responding countries are borne out in the reality of lower conviction rates for cybercrime offences – at least for this one example country. As discussed in the following section of this Chapter, in many developing countries, the prosecution of cybercrime offences faces the challenge not only of transnational evidence gathering and perpetrator obfuscation, but also of prosecutorial and judicial capacity and specialization limitations.

6.4 Criminal justice capacity

Key Results:

- Levels of prosecutorial cybercrime specialization are lower than for law enforcement authorities. Around 60 per cent of all responding countries have put in place specialized prosecutorial structures for cybercrime
- Developed countries show higher levels of prosecutorial specialization than developing countries
- Over 60 per cent of lesser developed countries reported that specialized prosecutors either had basic or no IT skills, and intermediate computer equipment or none at all
- Courts show minimal levels of specialization for cybercrime, with just 10 per cent of countries reporting specialized judicial services. The vast majority of cases are handled by non-specialized judges, who, in 40 per cent of responding countries do not receive any form of cybercrime-related training

In the same way as cybercrime and electronic evidence-based investigations require specialization within law enforcement, the prosecution and adjudication of cybercrime cases also calls for specialization within the criminal justice system. Such specialization requires personnel that have an understanding of concepts of computing and the internet, a knowledge of cybercrime legislative frameworks, and the ability to present and understand electronic evidence in court.

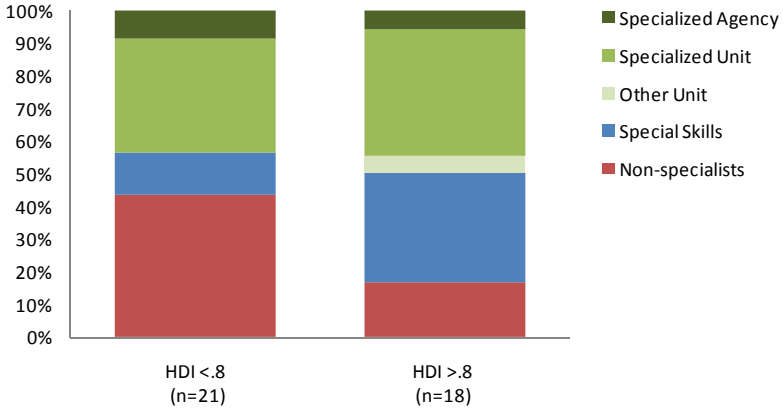
This section presents information reported by countries on the capacity of prosecutors and courts to prosecute and adjudicate cybercrime. As in Chapter Five (Law enforcement and investigations), institutional 'capacity' has a number of elements, including strategic and operational capabilities, technical skills of personnel, and sufficiency of personnel and resources; as well as degree of specialization. The point made in Chapter Five concerning an increasing need for *all* law enforcement officers to routinely handle and collect electronic evidence equally applies to prosecutors and judges. As the digital world advances, it may become hard to image the adjudication of *any* offence without the presentation and consideration of electronic evidence.

Organizational specialization

Country responses to the Study questionnaire show that the degree of organizational cybercrime specialization for prosecution authorities is significantly less than that reported for law enforcement agencies. Whereas more than 90 per cent of countries reported some degree of cybercrime specialization within law enforcement, this proportion drops to around 60 per cent for prosecution authorities, across all responding countries.[80] This figure conceals, however, significant differences according to levels of country development.

Almost 80 per cent of more highly developed countries report some form of prosecutorial cybercrime specialization. Around half of these countries have a specialized unit, while the other half have either a specialized agency, another specialized unit (such as for organized crime), or specialized personnel who are not organized in a separate unit. In contrast, less than 60 per cent of less developed countries report prosecutorial cybercrime specialization. In the majority of these, the degree of specialization is at the level of a specialized unit.

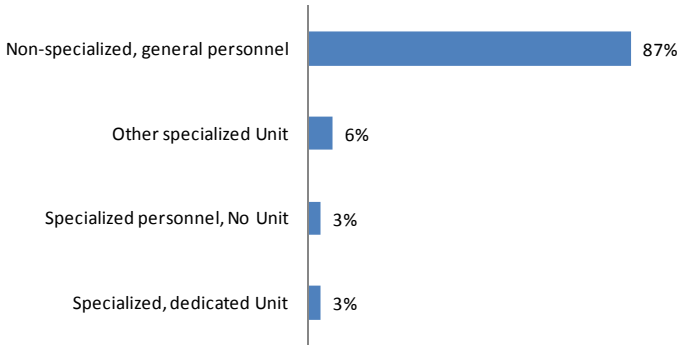
Figure 6.8: Prosecution structure for preventing and combatting cybercrime



Source: Study cybercrime questionnaire Q157. (n=41)

For developed countries reporting organizational specialization, many indicated that a specialized division or unit exists at the federal, provincial or state level in the ministry of justice or the national prosecution agency, frequently overseeing, coordinating or supporting specialized units or generalists in field and local offices. Some countries also reported technical and investigatory support from '*a dedicated team of police investigators, computer engineers and prosecutors that both investigate and prosecute cybercrime.*'[81] '*In some cases, individual prosecution offices have special competences to deal with prominent sets of proceedings related to information and communication crime, and for cybercrime in the strict sense.*' Another developed country noted that: '*There is some variation, but [a] small number of local offices have specialized internet child exploitation teams.*'[82]

Figure 6.9: Court structure for cybercrime cases



Source: Study cybercrime questionnaire. Q186. (n=31)

In less developed countries, arrangements are often less established. One country in Africa reported that its newly established unit was tasked with prosecution '*as well as advice on*

[80] Study cybercrime questionnaire. Q157.
[81] Study cybercrime questionnaire. Q157.
[82] *Ibid.*

policies and legislation, provide technical assistance to other prosecutors and law enforcement agencies, [but] as a new unit, training and equipment needs are yet to be met.'[83] In some, there is a reported '*lot of space for improvement.*' One country in Africa reported that *'There are no prosecutors assigned to do cybercrime cases. Any prosecutor is required to cover cybercrime even those who have not been trained on cybercrime.*'[84]

A few countries without specialized prosecution structures indicated plans to create a new prosecution structure for cybercrime. Such plans included proposals '*to create a number of specialized units*' and '*plans to create task forces in major cities that currently do not have specialized prosecution structures.*'[85] One country in Europe envisages creating '*independent units in prosecutors' offices with a great volume of activity and in the remaining offices to combine cyber specialized prosecutors with other types of specialized*'[86] units. Other countries reported no plans for a specialized unit, although some of these reported planning to integrate cyber-specialists into existing prosecutorial structures.

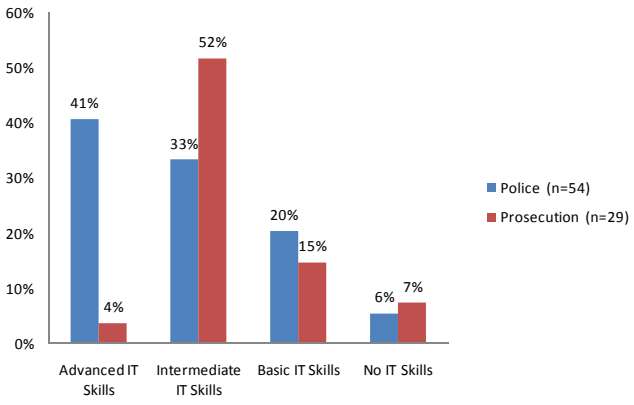
Court structures show the least degree of specialization, with around 10 per cent of all responding countries reporting some degree of court cybercrime specialization. Only three per cent of all responding countries reported a specialized, dedicated cybercrime judicial unit. Some six per cent reported another type of specialized judicial unit, such as a commercial crimes court. Three per cent reported the judicial oversight of cybercrime cases by specialized judicial personnel.

A few countries indicated that there are currently plans under way, either through legislation or administrative measures, to create specialized cybercrime courts or tribunals. In general, however, responding countries were of the view that they '*do not generally involve specialized courts based on thematic subject matter, although some judges at various levels do specialize in criminal cases as a matter of practice, and may tend to have criminal cases assigned to them by Chief Justices.*'[87]

Personnel specialization

In the same way as prosecution structures show less organizational specialization for cybercrime than law enforcement, so countries also reported lower levels of technical capabilities amongst specialized prosecutors than for law enforcement officers. Figure 6.10 shows country responses concerning law enforcement and prosecutorial IT skills.[88] While very few cybercrime prosecutors reported advanced IT skills compared with law enforcement officers specialized in cybercrime, this may, in part, reflect the different functional roles of each. Although prosecutorial involvement in investigations varies across legal systems, in general, law enforcement officers may be more often required to conduct or supervise initial forensics investigations and collection of electronic evidence.

Figure 6.10: Technical capabilities of police and prosecutors

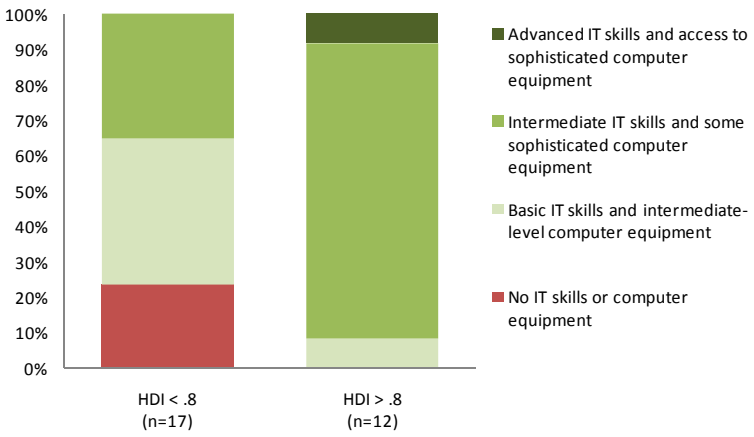


Source: Study cybercrime questionnaire. Q116 and Q160. (n=54, 29)

[83] *Ibid.*
[84] Study cybercrime questionnaire. Q160.
[85] Study cybercrime questionnaire. Q157.
[86] *Ibid.*
[87] Study cybercrime questionnaire. Q187.
[88] Study cybercrime questionnaire. Q116 and Q160.

Technical capabilities of prosecutors vary significantly by level of country development. More developed countries reported that around 80 per cent of prosecutors had intermediate IT skills and access to sophisticated equipment. Eight per cent had advanced IT skills. None of the developed countries reported that prosecutors did not have IT skills or computer equipment.

Figure 6.11: Technical capabilities of prosecutors



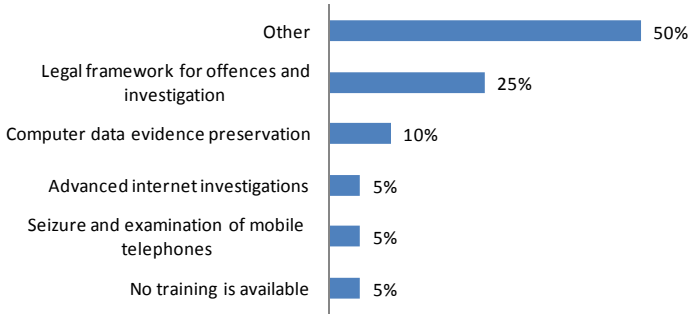
Source: Study cybercrime questionnaire. Q160. (n=29)

In contrast, over 60 per cent of less developed countries reported that specialized prosecutors either had basic or no IT skills, and intermediate computer equipment or none at all. These findings indicate significant gaps in capacity. In one less developed country, necessary computer equipment is '*available upon request,*'[89] although almost all countries reportedly face challenges in both training and equipment. '*Technical training is insufficient*' and more '*support in the area of training is needed to improve outcomes.*'[90] One more developed country reported '*Prosecutors have varying levels of advanced and intermediate IT skills, but have no access to sophisticated or even intermediate computer equipment.*'[91]

Personnel development

Reported training for specialized prosecutors covered a range of topics, with half of responding countries indicating that prosecutors were trained in multiple topics. In addition to the topics identified in Figure 6.12, others include '*operation of the Internet, types of cybercrime as well as investigations and jurisprudence*,'[92] information security, and '*preservation of electronic evidence with regard to money laundering offences.*' One country noted that '*Occasionally, prosecutors participate in the training that police organizations provide to their own experts.*'[93] Subject matter for training of specialized prosecutors is not as varied as that seen for law enforcement personnel and this

Figure 6.12: Training subject matters for specialized prosecutors



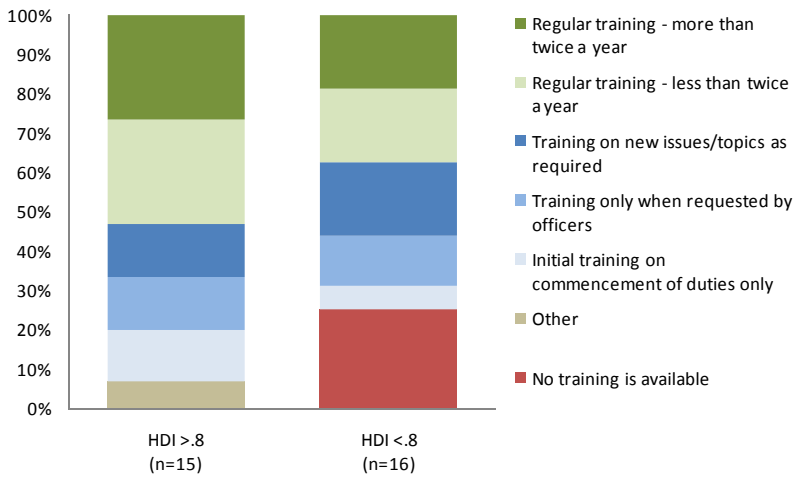
Source: Study cybercrime questionnaire. Q161. (n=20)

89 Study cybercrime questionnaire. Q160.
90 *Ibid.*
91 *Ibid.*
92 Study cybercrime questionnaire. Q161.
93 *Ibid.*

may be linked with differences in the roles of each within the criminal justice process. Several developing countries emphasized the need for more technical training for prosecutors. One country noted, for example, that '*Preparation in criminal law is of high quality, technical training is insufficient.*'[94] Another stated that '*We need more support in the area of training to improve outcomes.*'[95] Others emphasized that they '*require[d] more training in concepts such as information technology.*'[96]

Country responses also showed substantial variation in the frequency and duration of training for specialized prosecutors. Overall, over 40 per cent of responding countries reported that prosecutors received regular training, with just over 20 per cent reporting training more than twice a year. As with organizational specialization and technical capabilities, differences are also apparent by level of country development.

Figure 6.13: Frequency of training for specialized prosecutors

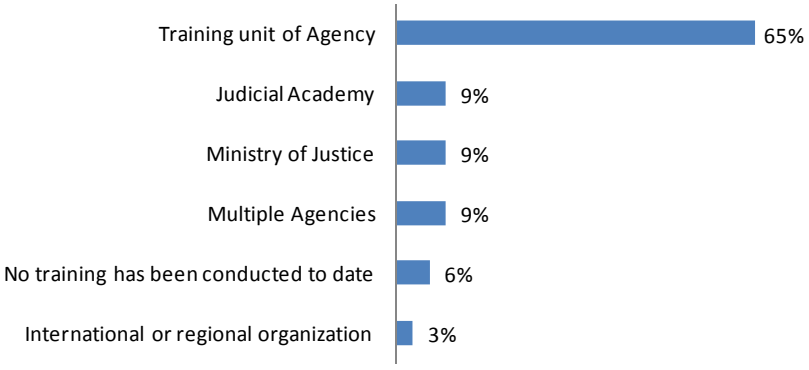


Source: Study cybercrime questionnaire. Q162. (n=31)

One quarter of specialized prosecutors in less developed countries do not have access to specialized training. Around 40 per cent receive regular training.

In contrast, none of the countries in the more developed cohort reported that no training was available, and over half of those countries reported that specialized prosecutors received regular training of more than once a year. Several more developed countries also detailed additional aspects related to training frequency including '*annual interdisciplinary training programs*,' '*e-learning modules*,' '*conference attendance*' and '*monthly training on specialized topics conducted by in-house and external experts*.'[97]

Figure 6.14: Training provider for specialized prosecutors



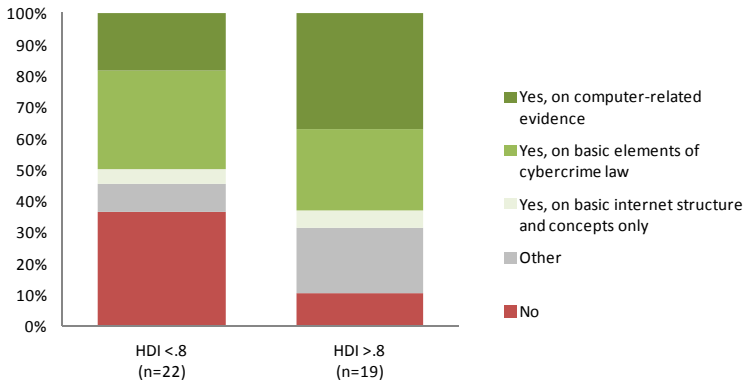
Source: Study cybercrime questionnaire. Q163. (n=34)

The most commonly reported training provider for specialized prosecutors was the training unit of the prosecution agency. Judicial academies and ministries of justice along with multiple agencies each constituted around 10 per cent of reported training providers for

94 Study cybercrime questionnaire. Q160.
95 *Ibid.*
96 *Ibid.*
97 Study cybercrime questionnaire. Q162.

prosecution specialists. A very small proportion – three per cent – of specialized prosecutors was reported to have been trained by international or regional organizations. Some six per cent of countries reported that no specialized training has yet been conducted for prosecutorial personnel.

Figure 6.15: Training for non-specialized prosecutors

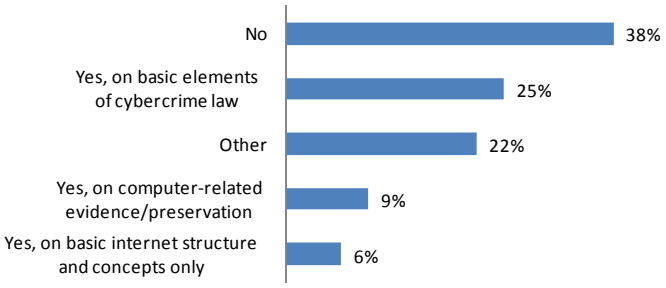


Source: Study cybercrime questionnaire. Q164. (n=41)

A number of responding countries recognized the importance of providing training on cybercrime also for *non*-specialist prosecutors. One country, for example, stated that '*During the last years, we have developed several activities in order to facilitate to all prosecutors an adequate knowledge of these* [*cybercrime*] *themes, with the purpose to provide them the best skills related to new technologies.*'[98] Another country highlighted that broader training was '*intended not only to enrich knowledge of legal doctrine of these crimes, but also seeks to raise awareness about the importance of adapting the classic procedural concepts to new technologies and forensic possibilities.*'[99] Overall, around 60 per cent of countries reported the existence of cybercrime training for non-specialized prosecutors. Figure 6.15 shows, however, differences by level of country development, with almost 40 per cent of lesser developed countries reporting that non-specialized prosecutors do not receive any form of cybercrime training.

Amongst the judiciary, around 40 per cent of all responding countries reported that no cybercrime-specific training is available for judges. One-quarter of responding countries reported training on basic elements of cybercrime law. Many countries' responses were similar to that of one Northern European country which commented that: '*Since there are no specialized judges, the training is covered by continuous training programmes organized by the magistracy which is open to all the magistrates. It is organized on an annual basis and usually has the duration of two days. This kind of training is rather of a general nature, such as an introduction to cybercrime.*'[100] One country reported judicial training '*aimed at covering cases based on national legislation on cybercrime, as well as summaries of recent cases.*'[101] In general, countries emphasized that a significant need exists for judicial training on '*cybercrime law, evidence collection, and basic and advanced computer knowledge.*'[102]

Figure 6.16: Cybercrime investigation training for non-specialized judges



Source: Study cybercrime questionnaire. Q192. (n=32)

98 Study cybercrime questionnaire. Q164
99 *Ibid.*
100 Study cybercrime questionnaire. Q189.
101 *Ibid.*
102 *Ibid.*

Such training as currently takes place was reported to be conducted by judicial training boards and centres, court and judicial training units, and ministries or institutes of justice. Several countries reported that judges may '*voluntarily elect to participate in professional development programs. Programs vary in the content they address and there is no prescribed training material for judges or magistrates involved in cybercrime cases.*'[103]

6.5 Capacity building and technical assistance

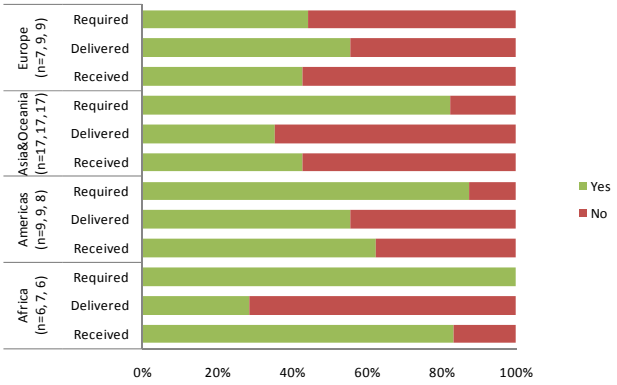
Key Results:

- 75 per cent of responding countries, across all regions of the world, reported requiring technical assistance in the area of cybercrime
- Technical assistance to date has mostly been delivered in the area of general cybercrime investigations and computer forensics and evidence. Reported need suggests that there is scope for assistance in the areas of international cooperation and prosecution, and trial support in particular
- A range of government institutions report requiring technical assistance, highlighting the need for a multi-disciplinary, holistic approach to cybercrime technical assistance
- The dominance of technical assistance activities lasting under one month indicates a clear need for longer term, sustainable investment

As a counterpart to the questions on the capacity of law enforcement, prosecution and court authorities to prevent and combat cybercrime, the Study questionnaire also included questions on needs for, and delivery of technical assistance by countries.

Overall, 75 per cent of responding countries, across all regions of the world, reported requiring technical assistance in some thematic area linked with cybercrime. Every responding country in Africa indicated a need for technical assistance.

Figure 6.17: Technical assistance required, delivered, and received



Source: Study cybercrime questionnaire. Q241, Q253, Q250 (n=40, 42, 39)

Over 70 per cent of all responding countries reported having provided some form of technical assistance to other countries, although less than 20 per cent of countries reported having received technical assistance. This could be indicative either of the fact that a large number of donor countries focus on a smaller number of recipient countries, or of the fact that a significant proportion of the world's least developed countries did not respond to the Study questionnaire.

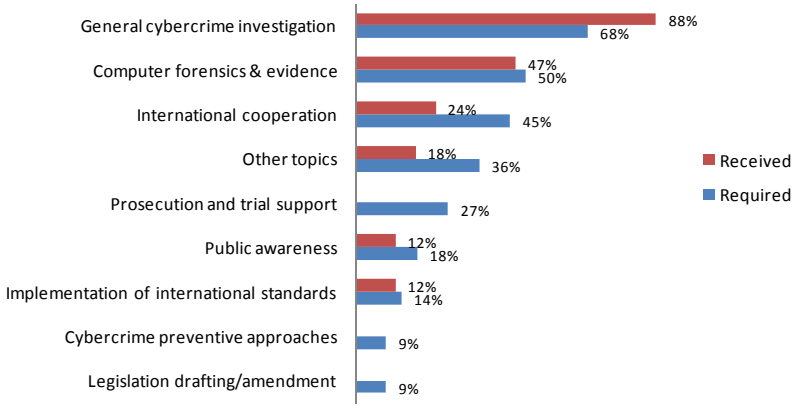
For European countries, just over half reported having received technical assistance, while less than half reported requiring or providing technical assistance in the area of cybercrime. In Asia, Oceania and the Americas, over 80 per cent of countries reported that they required technical assistance. A majority of countries in Asia and Oceania reported having provided technical

[103] Study cybercrime questionnaire. Q192.

assistance, and slightly less than half have received technical assistance. In the Americas, less than half have provided technical assistance while more than a third have received some form of technical assistance.

Topics - 'General cybercrime investigations' was the most commonly reported subject matter area for both technical assistance received and required, and the only subject matter area for which technical assistance was reported as received more often than reported as needed. This may suggest that there is scope for cybercrime technical assistance to move beyond a traditional focus on law enforcement investigations and to encompass a broader range of areas. In particular, the areas of 'international cooperation' and 'prosecution and trial support' represent fields in which assistance was reported to be required, but in which little was reported to have been delivered. One UN entity reported that '*Governments are requesting more training in these areas.*'[104]

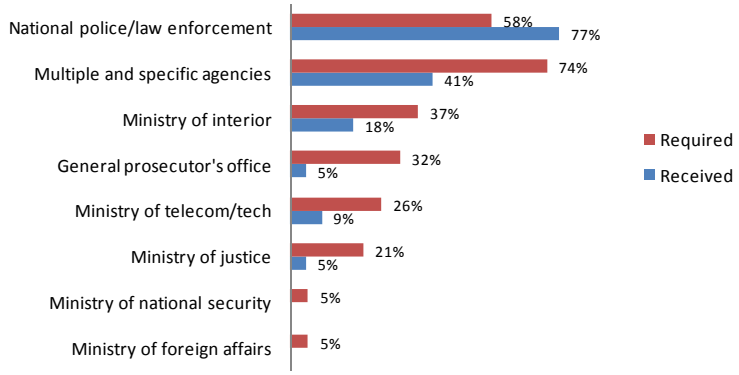
Figure 6.18: Technical assistance topics received and required



Source: Study cybercrime questionnaire. Q243 and Q251. (n=17, r=36; n=22, r=61)

Institutions – A large range of government authorities reported both requiring and receiving technical assistance – emphasizing the importance of a multi-disciplinary, holistic response to cybercrime. National police and law enforcement agencies reported having received technical assistance more frequently than requiring technical assistance. This may indicate the extent to which focus has been placed on strengthening capacity of law enforcement institutions as 'front line' responders to cybercrime. A higher level of reported delivery of technical assistance to law enforcement agencies may also correspond with reported higher levels of organizational and personnel specialization amongst law enforcement than for other criminal justice agencies (see Chapter Five (Law enforcement and investigations). Figure 6.19 also shows the relatively limited degree to which institutions such as prosecution offices and courts have received technical assistance, confirming the thematic picture in Figure 6.18.

Figure 6.19: Agencies requiring and receiving technical assistance



Source: Study cybercrime questionnaire. Q244 and Q252. (n=22, r=34; n=19, r=49)

[104] Study cybercrime questionnaire (IGO and academia). Q20.

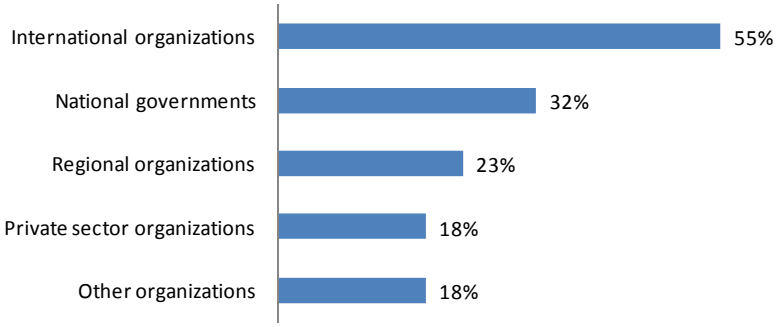
Delivery and donors - Governments were reported as the institution most frequently delivering technical assistance (over 75 per cent), followed by international organizations and international consultants. Regional organizations, such as the African Union, the Organization of American States, and the Council of Europe, were reported as providers of technical assistance by 20 per cent of responding countries. It should be noted, however, that 'delivery' structures for technical assistance may involve multiple modalities. The 'delivery' of a particular technical assistance programme or project, for example, may often be carried out through partnership between governments, and international or regional organizations, as well as independent consultants and academic organizations. Notably, international private sector organizations – with whom such partnerships also often exist – were reported to have delivered technical assistance to around 10 per cent of responding countries, highlighting the importance of private sector organizations as key partners in this area.

Figure 6.20: Institution delivering technical assistance

Source: Study cybercrime questionnaire. Q247. (n=17, r=35)

Responses from intergovernmental organizations to the Study questionnaire further highlighted the role that such organizations play in delivery of technical assistance. Organizations provide technical assistance on a variety of topics, from general investigation techniques, forensics and evidence preservation, to development of legislation, public-private cooperation, and international standard-setting and awareness-raising. A number of United Nations entities highlighted the importance of having a '*multilevel and holistic approach*' to technical assistance.[105] Many emphasized that it was important to build capacity in partnership, such as through '*networks of judicial training institutions*'[106] and using an approach such as '*train-the-trainer for IT crime investigators/examiners.*'[107] One organization, for example noted that it was important that '*all information and materials*' can be used by '*participants so as to provide the same training in their country domestically.*'[108] Depending on the focus of the programme, the target audience varies from the individual, such as law enforcement officers and forensic investigators, to the institutional, such

Figure 6.21: Organization or Donor supporting Technical Assistance Received



Source: Study cybercrime questionnaire. Q245. (n=22, r=32)

105 Study cybercrime questionnaire (IGO and academia). Q52.
106 *Ibid.*
107 *Ibid.*
108 *Ibid.*

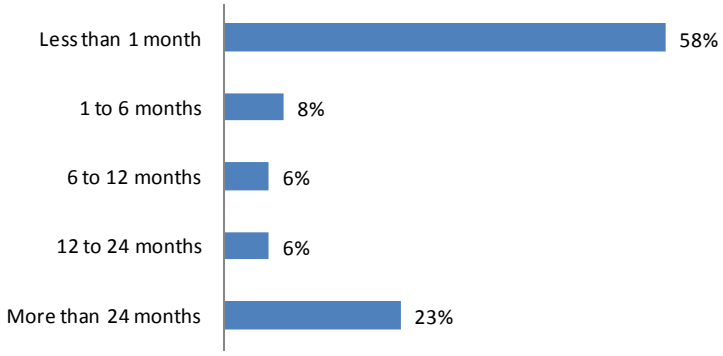
as ministries of interior, justice, and communication. International organizations have provided training in every region; most reported that training programmes are ongoing and in great demand, although sometimes constrained by resource availability.

A number of intergovernmental organizations raised the important question of *standards* and *certification*. One organization referred to the used of forensic training '*accredited by* [*a*] *University… delivered in 3 segments; a foundation level course in 2010, advanced courses in 2011, with an online Masters Degree pending for 2012.*'[109] One UN entity highlighted the challenge of identifying and knowing which professional standards should be followed and promoted during the delivery of training. The same entity reported, for example, that '*there is not yet any consensus on* [*forensic*] *curriculum requirements. As the field evolves there will likely be further course offerings and some standardization.*'[110] Other UN entities highlighted the challenge of a lack of resources and awareness concerning the problem of cybercrime as inhibiting the delivery of technical assistance. One UN entity indicated that '*We have the expertise but we don't have the resources to combat cybercrime.*'[111]

Support for technical assistance comes from a relatively small number of national governments, international, regional, and private sector organizations. The top reported support source for technical assistance was international organizations, with a majority (55 per cent) of countries indicating some form of technical assistance from this source. One UN entity indicated the importance of '*Training provided by experienced organizations in the region.*'[112] National governments were reported as the providing or supporting donor by almost one third of respondents while regional organizations accounted for almost one-quarter of support for technical assistance. Private sector and other types of organizations were reported as donors or sponsors for technical assistance by almost 20 per cent of respondents.

Duration – Almost 60 per cent of reported technical assistance programs lasted for less than one month. Only one quarter lasted for over two years. While technical assistance needs related to cybercrime may be all of long-term, medium-term, and short-term, the dominance of shorter-term technical assistance activities indicates a clear need for longer term, sustainable investment, that focuses on building core structural capacity of the range of government authorities and stakeholders involved in the cybercrime response.

Figure 6.22: Duration of technical assistance received



Source: Study cybercrime questionnaire. Q246. (n=24, r=52)

[109] *Ibid.*
[110] Study cybercrime questionnaire (IGO and academia). Q51.
[111] *Ibid.*
[112] Study cybercrime questionnaire (IGO and academia). Q52

Page left intentionally blank

CHAPTER SEVEN: INTERNATIONAL COOPERATION

This Chapter considers formal and informal international cooperation responses to the transnational challenge of cybercrime. It finds that widespread reliance on slow-moving traditional mechanisms such as mutual legal assistance, the emergence of country cooperation clusters, and a lack of clarity on permissible direct law enforcement access to extraterritorial data present challenges to an effective global response.

7.1 Sovereignty, jurisdiction and international cooperation

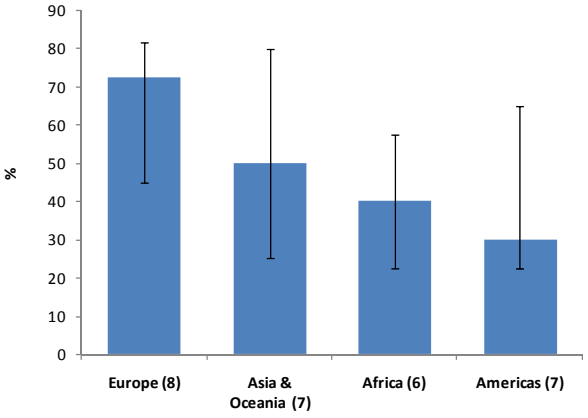
Key results:

- A 'transnational dimension' to a cybercrime offence arises where an element or substantial effect of the offence is another territory, or where part of the *modus operandi* of the offence is in another territory
- Countries responding to the Study questionnaire reported regional averages of between 30 and 70 per cent of cybercrime acts that involve a transnational dimension
- This engages issues of sovereignty, jurisdiction, transnational investigations, extraterritorial evidence, and a requirement for international cooperation

Cybercrime as a transnational crime

Cybercrime is by no means the first 'new' form of crime to demand a global response. Over the past decades, global action has been required to address challenges such as illicit drug trafficking and transnational organized crime, including through the development of international agreements. Nonetheless, it has become a truism that cybercrime today presents unique international cooperation challenges. During information gathering for the Study, more than half of countries reported that between 50 and 100 per cent of cybercrime acts encountered by the police involved a '*transnational element.*'[1] The figure shows that countries in Europe perceived the highest proportion of cybercrime acts involving a transnational dimension. Countries in Africa and the Americas perceived the lowest.[2]

Figure 7.1: Percentage of cybercrime acts involving a transnational dimension



Source: Study cybercrime questionnaire. Q83. (n=28)

One country from Eastern Europe noted that '*around 80 per cent of the cybercrime acts inspected by*

[1] Study cybercrime questionnaire. Q83. Some countries who could not provide exact numbers estimated the percentage to be 'very high.'

[2] The figure shows median values with upper and lower quartiles represented by error bars.

[*domestic law enforcement authorities*] *are related to more than one country.*'[3] Another, from West Africa, stated that most of the victims targeted by cybercrime perpetrators within its territory were located '*outside of national boundaries.*'[4] Other countries said that most reported offences were '*initiated outside*' of their territory. Still others observed that '*in most cases we act as a conduit.*'[5] Countries noted that the use of proxy servers, and the growing influence of social media, were among the factors behind an increasing number of cases involving a transnational dimension.[6] One country even reported that perpetrators are fully aware of jurisdictional issues and purposefully use internet resources, such as mail servers, located abroad in an attempt to hide evidence of their illegal activities.[7] The perception is not uniform however. One country from South America reported that a considerable number of reported transnational cases were '*of domestic origin.*'[8]

This Chapter examines jurisdictional and international cooperation approaches to combating cybercrime – both at the level of international and regional cybercrime instruments, as well as in the law and practice of states. It places information obtained from the Study questionnaire within the international legal framework of sovereignty, jurisdiction, and international cooperation in criminal matters.

The starting point - sovereignty and jurisdiction

The starting point for state jurisdiction and international cooperation is sovereignty. The sovereign equality of states is protected by rules of customary public international law. These include the obligation on states not to *'interfere in any form or for any reason whatsoever in the internal and external affairs of other States.'*[9]

Law enforcement and criminal justice matters fall within this exclusive domain of the sovereign state – with the result that, traditionally, criminal *jurisdiction* has been linked to geographical territory. States must therefore refrain from bringing pressure to bear on other states regarding the behaviour of specific national bodies, such as law enforcement agencies or the judiciary.[10] Persons may not be arrested, a summons may not be served, and police or tax investigations may not be mounted on the territory of another state, except under the terms of a treaty or other consent given.[11]

Of course, not all crimes occur neatly within the territorial jurisdiction. Where this is the case, international law has come to recognize a number of bases of *extra-territorial* jurisdiction in criminal matters.[12] Common bases found in national law and international agreements are summarized in the table below. Common to all of these principles is a broad sense of requirement that a 'sufficient connection' or 'genuine link' between the offence and the state exercising

---

3 Study cybercrime questionnaire. Q83.
4 *Ibid.*
5 *Ibid.*
6 *Ibid.*
7 *Ibid.*
8 *Ibid.*
9 As such, states have a right to sovereignty and territorial integrity, and to freely determine their own political, economic, cultural and social system, including all matters essentially within their domestic jurisdiction. See Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States, annex to GA resolution A/RES/20/2131 (XX), 21 December 1965. Please also refer to the *Corfu Channel* case, ICJ Reports 1949, 35, the *Military and Paramilitary Activities* case, ICJ Reports 1986, 202, and the *Nicaragua* case, ICJ Reports 1986, 14, 109-10.
10 Even, for example, where nationals of one state are on trial overseas, the basic underlying principle is that the state cannot interfere in the judicial procedures of the other sovereign state on behalf of its national. Similarly, states cannot take measures on the territory of another state by way of enforcement of their own national laws without the consent of the latter. See Cassese, A., *International Law*. p.53.
11 Brownlie, I., 2003. *Principles of Public International Law*. 6th ed. Oxford: Oxford University Press. p.306.
12 Jeschek, H. H., Weigend, T., 1996. *Lehrbuch des Strafrechts. Allgemeiner Teil.* 5th edn. Berlin: Duncker & Humbold. pp.167 et seq.

jurisdiction is needed.[13]

Principles of criminal jurisdiction	
Principle of territoriality (Objective territorial principle)	A state can prosecute activities upon its territory, even in cases where an offender is a foreign citizen If the perpetrator is outside of the territory, territorial jurisdiction nonetheless includes where one of the constituent elements of the offence, and more especially its effects, take place within the territory. The objective territoriality principle thus ensures that both the state where the behaviour commenced, and the state where the offence was concluded may validly try the alleged perpetrator[14]
Effects Doctrine	Jurisdiction is established over foreign conduct that produces substantial effects within the territory[15]
Principle of nationality **(Active)** **(Passive)**	Jurisdiction is established depending upon the nationality of the individual concerned[16] Jurisdiction is established based on the nationality of the offender, wherever the crime is committed Jurisdiction is established based on the nationality of the victim, wherever the crime is committed
Habitual residence	Jurisdiction is established based on the place of habitual residence of the offender[17]
Protective principle	Jurisdiction is established where a criminal act abroad is derogatory to the security of the state concerned and/or touches upon its vital interests[18]
Principle of universality	Jurisdiction is established over any person accused of committing a small number of 'international crimes,' such as piracy, war crimes and grave breaches of the Geneva Conventions, regardless of the territory or the nationality of individuals involved.[19] The principle is usually limited to situations where the state with territorial jurisdiction is unable or unwilling to prosecute

It is important to note that the use of such forms of jurisdiction by countries – either on the basis of national law or international agreements – does *not* automatically override the operation of sovereignty and non-interference principles. The physical conduct of a criminal investigation on foreign soil (under the protective principle or passive nationality principle, for example) still requires the consent of the foreign state.[20] The jurisdiction that a state claims to assert is thus related, but *separable*, from the question of non-interference and infringement of sovereignty.

International legal assistance regimes

In order to manage the process of consent for the conduct of law enforcement and criminal justice investigations outside a state's territory, a number of legal and informal arrangements exist between states, at the bilateral and multilateral level. Treaties concerning the formal surrender of suspected persons from one country to another, for example, are some of the oldest known

13 Epping, V. and Gloria, C., 2004. Der Staat im Völkerrecht. *In:* Ipsen, K., (ed.) *Völkerrecht.* 5th ed. Munich: C.H. Beck. pp.321-22.
14 *Lotus* case, PCIJ, Series A, No. 10, 1927, 23, 30.
15 See Hayashi, M., 2006. Objective Territorial Principle or Effects Doctrine? Jurisdiction and Cyberspace. *In Law* 6:285.
16 See Shaw, M., 2003. *International Law*. p.579 et seq. and Cassese, A., 2005. *International Law.* pp.451 et seq.
17 Jeschek, H. H., Weigend, T., 1996. *Lehrbuch des Strafrechts. Allgemeiner Teil.* 5th edn. Berlin: Duncker & Humbold. p.169.
18 Simma, B., Mueller, A., 2012. Exercise and the Limits of Jurisdiction. *In*: Crawford, J. and Koskenniemi, M., (eds.) *The Cambridge Companion to International Law*. pp.134,143.
19 Cassese, A., 2005. *International Law*. pp.451-452.
20 Brownlie, I., 2003. *Principles of Public International Law*. 6th ed. Oxford: Oxford University Press. p.306. For a national legal example of the prohibition of 'unlawful activities on behalf of a foreign State' see Art. 271, Swiss Criminal Code: '*Any person who carries out activities on behalf of a foreign State on Swiss territory without lawful authority, where such activities are the responsibility of a public authority of a public official… shall be liable to a custodial sentence.*' For a practical example of the approach of another to foreign criminal investigators, see: http://www.rcmp-grc.gc.ca/interpol/fcip-pcece-eng.htm

examples of international law.[21] Such 'extradition' treaties – as well as other forms of international cooperation (discussed below) – are typically worded carefully to ensure that their mechanisms respect the underlying principle of sovereignty. Article 4 of the Organized Crime Convention, for example, provides that '*States Parties shall carry out their obligations under this Convention in a manner consistent with the principles of sovereign equality and territorial integrity of States and that of non-intervention in the domestic affairs of other States*.' The Convention continues, to clarify that: '*Nothing in this Convention entitles a State Party to undertake in the territory of another State the exercise of jurisdiction and performance of functions that are reserved exclusively for the authorities of that other State by its domestic law*.'

In addition to extradition, the core tools of international cooperation include the provision of assistance in gathering evidence for use in criminal cases ('mutual legal assistance') and arrangements for the international transfer of sentenced persons.[22] Extradition can be defined as the formal process whereby a state requests the enforced return of a person accused or convicted of a crime to stand trial or serve a sentence in the requesting state.[23] *Customary* international law does not contain any general 'obligation to extradite.'[24] Arrangements are therefore usually based on bilateral or multilateral agreements, or reciprocity – the promise from one state to another to grant the same type of assistance in the future if asked to do so.[25] In order to avoid jurisdictional 'gaps', treaties commonly reflect a core principle of 'extradite or prosecute.'[26] Similarly, mutual legal assistance procedures are usually governed by multilateral – mostly regional[27] – or bilateral[28] agreements. Extradition and mutual legal assistance provisions within treaties may either be 'free-standing' in the sense that they apply to 'criminal matters' in general,[29] or restricted in scope by their inclusion in a subject-specific treaty.[30]

Where a state is party to such agreements, the procedure to be followed in processing both incoming and outgoing requests is often set out in national law. In addition, in some countries, domestic law may itself even provide a basis for international cooperation, in the place of reliance upon a treaty.[31] As one of the main aims of mutual legal assistance is to obtain evidence for use in criminal prosecutions and trials, the process is further inherently tied with national criminal procedure law. Evidence gathered abroad – often by the request*ed* state, and under its own procedures – will need to meet the evidentiary rules of the request*ing* state. These may include standards related to hearsay and continuity of an evidential 'chain of custody.'[32] In order to coordinate outgoing and incoming requests for extradition and mutual legal assistance, many states designate a 'central authority' with the power to receive requests and either to execute them or to transmit them to the competent authorities.[33] Article 18 of the Organized Crime Convention, for

---

21 Magnuson, W., 2012. The Domestic Politics of International Extradition. *Virginia Journal of International Law*, 52(4):839-891.

22 For an overview see UNODC, 2012. *Manual on Mutual Legal Assistance and Extradition*, and UNODC, 2012. *Handbook on the International Transfer of Sentenced Persons.*

23 *Ibid.* (*Manual on Mutual Legal Assistance and Extradition.* p.19).

24 *Lockerbie* case, Joint Declaration of Judges Evensen, Tarassov, Guillaume and Aguilar Maudsley, *ICJ Reports* 1992, 3:24.

25 UNODC, 2012. *Manual on Mutual Legal Assistance and Extradition.* p.23.

26 See Organized Crime Convention, Art. 16(10).

27 See, for example, Association of Southeast Asian Nations (ASEAN), 2004. *Treaty on Mutual Legal Assistance in Criminal Matters*; Council of Europe, 2000. *European Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union.*

28 For instance, Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the Argentine Republic concerning Mutual Judicial Assistance against Illicit Drug Trafficking, signed 27/08/1991, entry into force 01/06/1994; United States of America - Panama Treaty on Mutual Assistance in Criminal Matters, signed 04/11/1991, entry into force 09/06/1995.

29 See, for example, Agreement between the European Union and Japan on Mutual Legal Assistance in Criminal Matters. OJ L 39/20. 12 February 2010.

30 See, for example, United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances 1988, Art. 7, which provides that States Parties shall afford assistance '*in relation to criminal offences established in accordance with article 3, paragraph 1.*' The relevant offences concern the production, manufacture, extraction etc. of narcotic drugs and psychotropic substances.

31 UNODC, 2012. *Manual on Mutual Legal Assistance and Extradition,* p.22.

32 *Ibid.* p.15. See also Chapter Six (Electronic evidence and criminal justice).

33 See Study cybercrime questionnaire. Q195 (extradition) and Q217 (mutual legal assistance).

example, requires States Parties to designate a central authority for mutual legal assistance requests.[34]

An evolving alternative to mutual legal assistance is the principle of *mutual recognition* in criminal investigative matters. Traditional mutual legal assistance typically requires lengthy verification of the validity of the request – including with respect to whether the conduct which is the object of the request is an offence under the domestic law of the requested state.[35] Mutual recognition between states aims to create a simplified, accelerated procedure with limited possibilities to refuse requests, founded on the principle of mutual trust in criminal justice systems and unity of laws. Its successful operation requires minimum rules concerning the definition of criminal offences and sanctions, as well as harmonized possibilities for the protection of individual rights.[36] In the European context, the framework for mutual legal assistance is accompanied by an emerging trend towards mutual recognition – including through the development of a European arrest and evidence warrant, and proposals for a 'European investigative order.'[37]

In addition to forms of formal international cooperation, parts of the process of extra-territorial law enforcement investigations may be undertaken by *informal* police-to-police or agency-to-agency communication. Such communication can be used *prior* to a formal mutual legal assistance request to a competent authority, or to *facilitate* a formal request. Where informal police-to-police networks are used in matters such as locating witnesses or suspects, conducting interviews, or sharing police files or documentation, two particular concerns are: (i) that the request is not perceived in the requested state as an attempt to conduct foreign criminal investigations without the proper consent; and (ii) that any evidence obtained for use in prosecution or trial still meets the evidentiary standards of the requesting state, including chain of custody requirements.[38]

In addition to the network of informal bilateral relationships between law enforcement agencies, INTERPOL maintains a system of national central bureaus in 190 countries. Bureaus are typically designated sections with the national law enforcement agency.[39] Through an online 'I-24/7' system, bureaus may facilitate either bilateral or multilateral informal police-to-police requests, or the transmission of a *formal* mutual legal assistance request from one central authority to another – via the national central bureaus.[40]

What is a 'transnational dimension'?

The common perception of cybercrime as involving a transnational 'dimension' calls for careful analysis. When, and how, for example, can a cybercrime offence be said to involve a transnational dimension? One starting point is the approach of the United Nations Organized Crime Convention – which provides that an offence is '*transnational in nature*' if: (i) it is committed in more than one state; (ii) it is committed in one state but a substantial part of its preparation, planning, direction or control takes place in another state; (iii) it is committed in one state but involves an

---

34 Organized Crime Convention, Art. 18(13). A directory of competent authorities appointed in accordance with the Organized Crime Convention and its Protocols, as well as the United Nations Convention against Illicit Trafficking in Narcotic Drugs and Psychotropic Substances of 1988, is maintained at www.unodc.org/compauth

35 See Organized Crime Convention, Art. 18(9).

36 In the European context see, for instance, The Stockholm Programme. OJ C115, 4 May 2010. 1-38.

37 See Council Framework Decision 2008/978/JHA of 18 December 2008 on the European evidence warrant for the purpose of obtaining objects, documents and data for use in proceedings in criminal matters; and Initiative of the Kingdom of Belgium and others regarding the European Investigation Order in criminal matters. OJ C165/22. 24 June 2010. See also European Union Agency for Fundamental Rights, 2011. *Opinion of the European Union Agency for Fundamental Rights on the draft Directive regarding the European Investigation Order.*

38 UNODC, 2012. *Manual on Mutual Legal Assistance and Extradition.* pp.66-67.

39 See http://www.interpol.int/About-INTERPOL/Structure-and-governance/National-Central-Bureaus

40 UNODC, 2012. *Manual on Mutual Legal Assistance and Extradition.* p.31.

organized criminal group that engages in criminal activities in more than one state; or (iv) it is committed in one state but has substantial effects in another state.[41]

The approach contains many important features – including the principle of 'substantial effects' within a state. When it comes to cybercrime acts, however, it may not offer a complete approach. As discussed in the section on 'Cybercrime perpetrators' in Chapter Two (The global picture) of this Study, there is no reason why 'organized criminal groups' should be central to cybercrime acts.[42] In addition, due to the global movement of data in internet transactions, a transnational 'dimension' may arise that does not amount to 'preparation, planning, direction or control' within another state.

An approach for cybercrime is to recognize that the determination of a 'transnational dimension' makes most sense when examined with reference to considerations of (i) *jurisdiction*; and (ii) criminal *evidence*. One method of characterizing *any* offence, for example, is to differentiate the act *elements* of '*conduct*', '*circumstance*', and '*result*.'[43] Where one or more of these elements occurs in, or produces substantial effects within,[44] another territorial jurisdiction, a 'transnational dimension' will exist. As discussed below, this will, in turn have implications for jurisdictional claims. Under this approach, a single '*location*' of a cybercrime offence *per se* may not be determinable – or, indeed, relevant. Rather, what matters is the successful identification of elements or substantial effects that allow a state to establish jurisdiction – subject always to the requirement of a 'sufficient connection'.

In addition, from a broader perspective, a cybercrime transnational 'dimension' may arise where part of the *modus operandi* of the offence occurs in another jurisdiction. The mere presence in extra-territorial servers of computer data related to the offence, for example, might not (depending upon local law) be sufficient to engage the *jurisdiction* of the server country. It would, however, be highly relevant for *evidence* and the investigative process of any country claiming jurisdiction – possibly requiring action such as a mutual legal assistance request to the server country. In this situation, a cybercrime case might also be said to have a transnational 'dimension'. A high number of cybercrime cases likely fall within this category. They may not, however, always be characterized as such – either due to sufficient evidence within the prosecuting jurisdiction, or a failure to identify extra-territorial evidence in the first place.

Two themes are particularly important when it comes to the extra-territorial 'evidence' dimension: (i) the increasing involvement of electronic evidence in *all* crime types and not just those falling within the term 'cybercrime'; and (ii) the increasing use of cloud computing involving distributed and parallel data storage. In particular, automated dynamic data placement within cloud services in data centres physically located in different countries may present challenges to the identification of data 'location.'[45] Following an examination of how international and national

---

41 Organized Crime Convention, Art. 3(2).

42 Although in practice many may be involved. See Chapter Two (The global picture), Section 2.3 Cybercrime perpetrators, Role of organized criminal groups.

43 Fletcher, G., 1978. *Rethinking Criminal Law*. Oxford: Oxford University Press. Thus, for example, an offence of 'computer system interference' may require the 'intentional' (intent) 'damaging, deleting, altering or suppressing of computer data' (conduct) 'seriously hindering' (result) the 'functioning of a computer system' (circumstance).

44 Operation of the 'effects doctrine' has been argued to represent an extension of the objective territorial principle, in so far as it does not require an 'element' of the offence to be located within the jurisdiction. See, for example, *Ahlstrom and Others v Commission of European Communities* [1988] ECR 5193. In the cybercrime context, a review of jurisdictional principles relied upon by national courts in extra-territorial cases suggests that '*whichever characterization* [objective territoriality or effects doctrine] *a municipal court chooses to rely on*, *the extent of jurisdiction justified will be the same*.' See Hayashi, M., 2006. Objective Territorial Principle or Effects Doctrine? Jurisdiction and Cyberspace. *In: Law* 6:284-302, p.285.

45 See, for example, Peterson, Z.N.J., Gondree, M. and Beverly, R., 2011. A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud. *In: Proceedings of the ACM Conference on Data and Application Security and Privacy* (CODASPY). For an

approaches address transnational aspects of cybercrime in general, this Chapter concludes with a particular focus on obtaining extra-territorial evidence from individuals and third party service providers.

7.2 Jurisdiction

Key results:

- International law provides for a number of bases of jurisdiction over cybercrime acts, primarily including forms of territory- and nationality-based jurisdiction
- Some of these bases can be found in multilateral cybercrime instruments
- While all countries in Europe consider that national laws provide a sufficient framework for the criminalization and prosecution of extra-territorial cybercrime acts, around one-third to one-half of countries in other regions of the world report insufficient frameworks for extraterritorial cybercrime acts
- In many countries, provisions reflect the idea that the 'whole' offence need not take place within the country in order to assert territorial jurisdiction. Territorial linkages can be made with reference to elements or effects of the act, or the location of computer systems or data utilized for the offence
- Where they arise, jurisdictional conflicts are typically resolved through formal and informal consultations between countries
- Country responses do not reveal, at present, any need for additional forms of jurisdiction over a putative 'cyberspace' dimension. Rather, forms of territoriality-based and nationality-based jurisdiction are almost always able to ensure a sufficient connection between cybercrime acts and at least one State

This section examines the jurisdictional approach of both international and regional cybercrime instruments and countries. As discussed in Chapter Three (Legislation and frameworks) of this Study, a number of international and regional cybercrime instruments contain jurisdiction provisions. Instruments typically specify that States parties shall adopt legislative and other measures to provide for certain forms of jurisdiction over offences established in accordance with the instrument.[46] The table below summarizes jurisdiction provisions in key binding and non-binding international and regional cybercrime instruments. Further details and article numbers are also included in the table at Annex Three to this Study.

example of automated data placement technology across geo-distributed data centres, see Agarwal, S., *et al.*, 2010. *Volley: Automated Data Placement for Geo-Distributed Cloud Services*. NSDI.

[46] See, for example, Council of Europe Cybercrime Convention, Art. 22.

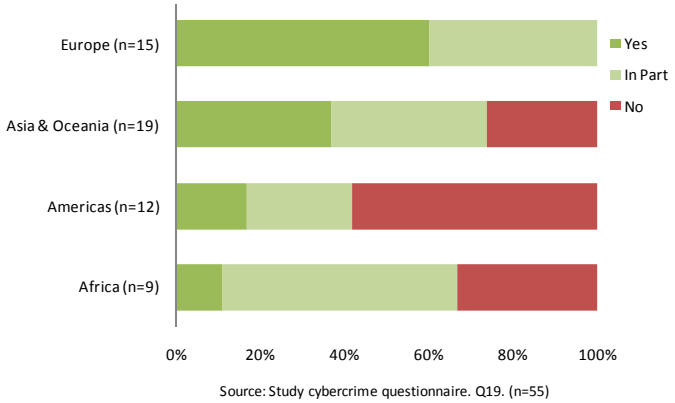
Jurisdiction provisions in international and regional cybercrime instruments								
	Binding instruments					Non-binding instruments		
Grounds for Jurisdiction	**Draft African Union Convention**	**Commonwealth of Independent States Agreement**	**Council of Europe Cybercrime Convention**	**League of Arab States Convention**	**Shanghai Cooperation Organization Agreement**	**COMESA Draft Model Bill**	**Commonwealth Model Law**	**ITU/CARICOM/ CTU Model Legislative Texts**
Territory-based jurisdiction								
Territorial	–	–	■	■	–	■	■	■
Directed against computer system/data in territory	–	–	–	–	–	■	–	–
Ships/Aircrafts	–	–	■	■	–	■	■	■
Nationality-based jurisdiction								
Active	–	–	■	■	–	■	■	■
Passive	–	–	–	–	–	–	–	–
Other jurisdiction								
Habitual Residence	–	–	–	–	–	–	–	–
State interests	–	–	–	■	–	–	–	–
When extradition refused	–	–	■	■	–	■	–	–
Additional provisions								
Rules on concurrent jurisdiction	–	–	■	■	–	■	–	–

The details of individual provisions are examined below, together with relevant examples and practices from information reported by countries through the Study cybercrime questionnaire.

Prosecuting extra-territorial offences

During information gathering for the Study, countries were asked about the perceived sufficiency of their national legal frameworks for the criminalization and prosecution of cybercrime acts committed outside of their country.[47] Figure 7.2 shows that the general picture is one of a reasonable degree of sufficiency, but with marked regional differences. Around one-third of total responding countries perceived their national legal framework for extra-territorial offences to be 'sufficient.' A further 40 per cent considered it to be sufficient 'in part.' Twenty-five per cent reported that it was 'not sufficient.'[48] Frameworks were perceived to be least sufficient in the Americas, where only 40 per cent of countries reported that their legal frameworks were sufficient or partly

Figure 7.2: Does national law provide a sufficient framework for criminalization and prosecution of cybercrime acts committed outside of country?



Source: Study cybercrime questionnaire. Q19. (n=55)

47 Study cybercrime questionnaire. Q19.
48 *Ibid.*

sufficient, compared with around 67 per cent of countries in Africa, Asia and Oceania. All responding countries from Europe – all except one of which had either signed or ratified the Council of Europe Cybercrime Convention – considered their legislation to be sufficient or partly sufficient.

Countries that did not consider their legislation to be sufficient for extra-territorial acts cited a number of reasons. Common gaps included either a lack of provisions in criminal codes addressing acts committed outside of the jurisdiction, as well as, in some cases, the non-applicability of extradition and mutual legal assistance legislation to cybercrime acts.[49]

Country responses to the Study questionnaire showed that grounds for jurisdiction in extra-territorial cybercrime cases are primarily based on principles such as territoriality (including as interpreted by the objective territoriality principle and substantial effects doctrine) and the nationality of the offender.[50] As such, states generally require some degree of internal effect, such as victimization of nationals or effects or damage within the territory. Respondent countries often reported that if the crime is committed *entirely* outside of the country, with no effects within the territory, then criminalization and prosecution can be particularly challenging.

Common national bases for jurisdiction in cybercrime cases

Territory

- Commission of crime partly/wholly on the territory
- Effects/damages within the territory
- Computer/programme/data used for the commission of the crime located within the territory
- Commission on registered ships and aircrafts (including military)

Nationality

- Active – Offender
- Habitual residence
- Passive – Victim

Other criteria

- State interests are affected
- *Ne bis in idem*

Using territorial jurisdiction

International and regional instruments – All international or regional cybercrime instruments that contain a jurisdiction clause recognize the territorial principle – requiring States parties to exercise jurisdiction over any offence established in accordance with the instrument, that is 'committed' within the state's geographical territory.[51] Criminal activities on ships and aircrafts are also covered by a number of binding and non-binding instruments.[52]

In accordance with the objective territoriality principle, many international and regional instruments recognize that is not necessary for *all* elements of the offence to occur within the territory in order for territorial jurisdiction to apply. The Council of Europe Cybercrime Convention Explanatory Report, for example, clarifies that under the principle of territoriality, a party would assert territorial jurisdiction if both the person attacking a computer system and the victim system are located within its territory, '*and where the computer system attacked is within its territory, even if the attacker is not.*'[53]

The COMESA Draft Model Bill includes a provision in the instrument itself on the '*place*

---

49 *Ibid.*

50 Study cybercrime questionnaire. Q18 and Q19.

51 See, for example, Council of Europe Cybercrime Convention, Art. 22(1)(a); League of Arab States Convention, Art. 30(1)(a); UN OP-CRC-SC, Art. 4(1); COMESA Draft Model Bill, Art. 40(a)(1); ITU/CARICOM/CTU Model Legislative Text, Art. 19(a); Commonwealth Model Law, Art. 4(a).

52 See, for example, COMESA Draft Model Bill, Art. 40(b); Commonwealth Model Law, Art. 4(b); Council of Europe Cybercrime Convention, Art. 22(1)(b), (c); Council of Europe Child Protection Convention, Art. 25(1)(b), (c); ITU/CARICOM/CTU Model Legislative Texts, Art. 19(b); League of Arab States Convention, Arts. 30(1)(b), (c); and United Nations OP-CRC-SC, Art. 4(1).

53 Council of Europe, 2001. *Explanatory Report to Convention on Cybercrime.*

where the offence occurred.'[54] One component of this provision includes: *'[an offence is committed]… (iii) at any location which the resulting action is an element of an offence pursuant to… this Law occurred or would have occurred.*'[55] The EU Directive on Child Exploitation requires jurisdiction where the offence is committed in whole '*or in part*' within the territory. It clarifies that this includes where the offence is committed by means of information and communication technology '*accessed from*' the territory *'whether or not*' the technology is based in the territory.[56] The EU Decision on Attacks against Information Systems covers both attacks committed by an offender physically present on the territory (whether or not against an information system on the territory), and attacks against information systems on the territory (whether or not the offender is physically present on the territory).[57]

National approaches – The influence of territoriality approaches in international and regional instruments is seen at national level. Countries reported a range of provisions reflecting the idea that the 'whole' offence need not take place within the country in order to assert territorial jurisdiction. Mechanisms varied, however, for identifying the existence of a territorial connection.

Example of cyber-specific legislation covering territorial jurisdiction in cybercrime cases from a country in Southern Africa

Jurisdiction of courts.
A court in the Republic trying an offence in terms of this Act has jurisdiction where—

(a) the offence was committed in the Republic;
(b) any act of preparation towards the offence or any part of the offence was committed in the Republic, or where any result of the offence has had an effect in the Republic;
(c) …
(d) the offence was committed on board any ship or aircraft registered in the Republic or on a voyage or flight to or from the Republic at the time that the offence was committed.

In some cases, these focused on the 'act.' In other cases, they focused on the location of 'computer systems and data.'[58] Some countries reported, for example, that territorial jurisdiction included crimes that are initiated, continued or completed elsewhere, but are either partly '*carried out,*' or '*affect*' property, or '*cause*' personal harm, within the state territory.[59] Other countries referred to the assertion of jurisdiction where '*server or hardware utilized for the commission of the crime*' is located outside of the territory, but where there is '*some kind of domestic effect or element.*'[60]

Examination of case law also shows that national courts have claimed jurisdiction where all of the *elements* of a crime are within the country, *except* for the *result* (in this case, harm to an extra-territorial victim receiving harassing messages).[61] Conversely, law enforcement authorities have also issued indictments where the crime *result* (of illegal access and fraudulent loss) was within the country, but the *conduct* and location of the perpetrators was extra-territorial.[62] Countries observed that such concepts had been applied to cases involving internet gambling and child pornography.[63] A small number of countries from Europe and the Americas reported, however, that national legislation was insufficient to address some *specific* extra-territorial cybercrime acts – including denial of service, sending of spam, and phishing attacks.[64]

54 COMESA Draft Model Bill, Art. 40(f).
55 *Ibid.* Art 40(f)(iii).
56 EU Directive on Child Exploitation, Art. 17.
57 EU Decision on Attacks against Information Systems, Art. 10.
58 Study cybercrime questionnaire. Q18.
59 *Ibid.*
60 *Ibid.*
61 *DPP v. Sutcliffe* [2001] VSC 43. 1 March 2001.
62 *US v Tsastsin et al.* United States District Court. Southern District of New York. S2 11 Cr. 878.
63 Study cybercrime questionnaire. Q18.
64 Study cybercrime questionnaire. Q19.

Many countries stated that they would not have jurisdiction over an act carried out, *and* taking effect, entirely outside of the territory. One country in Asia, however, reported that it could assert jurisdiction in such circumstances if computer systems or other equipment used in the offence were located on its territory.[65] While a conceptual distinction exists between 'offence elements and effects,' and 'computer systems used in the offence', it is likely that there is significant overlap between these two approaches – in particular where the use of computer systems can be characterized as part of the 'conduct' or 'circumstance' offence elements.

Finally, some countries noted the constraints of nationality on territoriality. Even where territorial jurisdiction could be asserted – such as when an extra-territorial act is covered by the effects doctrine – many countries reported that the situation was unclear if the extra-territorial perpetrator was a *foreign* national. Several countries noted that they only initiated proceedings when additional requirements are met.[66] In one country, for example, criminalization and prosecution of such foreign suspects depends on whether the offence significantly harms its interests and internal security.[67] A small number of countries in Asia and the Americas reported allowing for jurisdiction over offenders of any nationality, regardless of the place where the offence itself is committed – as long as some link could be established, such as the presence of the perpetrator, or the device or data utilized in the offence, within the territory at the material time, or the occurrence of damage within the territory.[68] For the situation where an alleged foreign perpetrator remains physically present in the territory, some countries referred to the obligation to 'extradite or prosecute.'

Example of legislation that specifically extends territorial jurisdiction to non-nationals from a country in the Caribbean

(1) Subject to subsection (2), this Act shall have effect in relation to any person, whatever his nationality or citizenship, outside as well as within the State, and where an offence under this Act is committed by a person in any place outside of the State, he may be dealt with as if the offence had been committed within the State.
(2) For the purpose of subsection (1), this Act shall apply if, for the offence in question—
(a) the accused was in the State at the material time;
(b) the computer, program or data was in the State at the material time; or
(c) the damage occurred within the State, whether or not paragraph (a) or (b) applies.

Using nationality-based jurisdiction

International and regional instruments – Where international or regional cybercrime instruments recognize the territoriality principle, they frequently also include the active nationality principle – requiring a state to ensure jurisdiction when the act has been committed by one of its nationals, including outside of the national territory.[69] Some instruments require that the national's conduct is also criminalized in the country where it occurred.[70]

Only a limited number of instruments provide for jurisdiction based on the passive nationality principle – notably those that concern the rights of children. The EU Directive on Child Exploitation, and the United Nations OP-CRC-SC require states to establish jurisdiction over an offence committed outside of the territory against '*one of its nationals,*' or a person who is a '*habitual*

65 Study cybercrime questionnaire. Q18.
66 *Ibid.*
67 *Ibid.*
68 For instance, see Computer Crimes Act of Malaysia (1997), Art. 9; Computer Misuse Act of Singapore (Revised, 2007), Art. 11; Computer Misuse Act of Trinidad and Tobago (2000), Art. 12.
69 See, for example, Council of Europe Child Protection Convention, Art. 25(1)(d), and EU Directive on Child Exploitation, Art. 17(1)(b).
70 See COMESA Draft Model Bill, Art.40(c); Commonwealth Model Law, Art. 4(d); Council of Europe Cybercrime Convention, Art. 22(1)(d); and League of Arab States Model Law 2004, Art. 30(1)(d).

resident'.[71] The Council of Europe Child Protection Convention provides that States parties shall '*endeavour*' to establish such jurisdiction.[72] Such provisions offer countries the jurisdictional power to ensure the protection of national children abroad.

National approaches – A number of countries referred to the use of the active nationality principle in order to assert jurisdiction over offences committed by their nationals, wherever they are committed. Although not a common requirement, a few countries noted that there was a requirement for the act to also constitute an offence in the state in which it was committed.[73]

A few countries also referred to the passive nationality principle for jurisdiction over offences affecting nationals, wherever they occur. One country in Europe, for example, reported that many cybercrime cases it encountered had extra-territorial elements and that in some cases, national victims were located abroad – creating jurisdictional complications.[74] Another country in Europe reported that it had adopted a new criminal code that included the passive nationality principle specifically in order to reduce jurisdictional difficulties in cases where the offender is a foreigner who commits a crime abroad that affects a national outside of the territory.[75]

Using other bases of jurisdiction

International and regional instruments – Two instruments, the League of Arab States Convention and Model Law, specifically provide for the protective principle. The Convention, for example, specifies that States parties shall extend competence over offences affecting '*an overriding interest of the State.*'[76] European instruments, including the EU Decision on Attacks against Information Systems, also include an additional basis of jurisdiction covering offences committed for the benefit of a '*legal person*' that has its head office within the territory.[77] Finally, in accordance with the principle of 'extradite or prosecute,' a number of instruments provide for jurisdiction where an alleged offender is present in the territory and the state does not extradite him or her to another state, solely on the basis of his or her nationality, after a request for extradition.[78]

National approaches – A few responding countries made reference to the protective principle in the context of conditions attached to other forms of jurisdiction. As regards other jurisdictional bases, such as universal jurisdiction, a number of countries referred to the situation where a foreign perpetrator of an entirely extra-territorial offence is found in the territory, but there is no request for extradition. Some countries noted that universal jurisdiction was limited to genuine international crimes and did not generally cover cybercrime acts.[79] Others, however, proposed that some grave cybercrime acts, such as child pornography, arguably could fall within such a form of jurisdiction.[80]

---

71 EU Directive on Child Exploitation, Art. 17(2)(a), and United Nations OP-CRC-SC, Art. 4(2)(b).
72 Council of Europe Child Protection Convention, Art. 25(2).
73 Study cybercrime questionnaire. Q18.
74 Study cybercrime questionnaire. Q19.
75 *Ibid.*
76 League of Arab States Convention, Art. 30(1)(e).
77 EU Decision on Attacks against Information Systems, Art. 10(1)(c); EU Directive on Child Exploitation, Art. 17(2)(b); EU Decision on Fraud and Counterfeiting, Art. 9(1)(c); and EU Directive Proposal on Attacks against Information Systems, Art. 13(1)(c).
78 COMESA Draft Model Bill, 2011, Art. 40(d); Council of Europe Cybercrime Convention, Art. 22(3); Council of Europe Child Protection Convention, Art. 25(7); EU Decision on Attacks against Information Systems, Art.10(3); EU Decision on Fraud and Counterfeiting, Art. 10(1); League of Arab States Convention, Art. 30(2); United Nations OP-CRC-SC, Art.4(3).
79 Study cybercrime questionnaire. Q18.
80 *Ibid.*

Jurisdictional conflicts

International and regional instruments – Operation of the range of jurisdictional bases by different countries can lead to the situation where more than one country asserts jurisdiction over a particular cybercrime act. A number of the international and regional instruments address this 'concurrent' jurisdiction challenge. Some specify, for example, that where an offence falls within the jurisdiction of more than one state and when any of the states concerned can validly prosecute on the basis of the facts, states must 'cooperate' or 'consult' in order to decide the most appropriate jurisdiction for prosecution.[81] The European instruments, in particular, aim at '*centralising proceedings in a single* [*state*].'[82] The League of Arab States Convention provides a detailed order of priority for competing jurisdictional claims as follows: (i) states whose security or interests have been disrupted by the offence; (ii) states in whose territory the offence was committed; and (iii) the state of nationality of the offender. If no balance can be found according to this order, then priority is accorded to the first requesting state. [83]

National approaches – During information gathering for the Study, countries reported that, in general, they did not have specific legislation intended to resolve conflicts of jurisdiction in cybercrime cases.[84] Nonetheless, a number of countries mentioned plans to address possible conflicts of jurisdiction in cyber-specific legislation by means of legal surveys or policy positions. One country, however, noted that, as far as transnational cybercrime was concerned '*the range of possible cases and scenarios may make it difficult, and possibly inadvisable, to develop concrete universal legal rules based on jurisdictional exclusivity*.'[85]

Countries reported resolving jurisdictional disputes by relying on formal and informal consultations with other countries in order to avoid double-investigations and jurisdictional conflicts.[86] As one country in Europe noted, '*[m]ost of the time such conflicts of jurisdiction can be avoided through informal prior consultation, or spontaneous exchange of information. Also joint investigation operations can contribute […]*.'[87] Communication is conducted bilaterally, or through channels made available by institutions such as INTERPOL, Europol and Eurojust.[88] One country from the Americas indicated that, since the prosecution of these fragmented crimes was highly difficult, proceedings would essentially only be initiated when there was a strong indication that either the offender or the victim was one of its citizens. All other cases would be communicated to the countries of origin via INTERPOL channels.[89] In addition, a number of countries referred to the principle of *ne bis in idem* ('not twice'), and will only initiate proceedings if none are conducted in the country where the acts were committed. Before giving up their claim on jurisdiction, some countries require assurances that the other state claiming jurisdiction will adhere to human rights standards during investigations and proceedings.[90]

---

81 Council of Europe Child Protection Convention, Art. 25(8); Council of Europe Cybercrime Convention, Art. 22(5); EU Decision on Attacks against Information Systems, Art. 10(4); and COMESA Draft Model Bill, Art. 40(e).
82 See, for example, EU Decision on Attacks against Information Systems, Art. 10(4).
83 League of Arab States Convention, Art. 30(3).
84 Study cybercrime questionnaire. Q18.
85 *Ibid.*
86 *Ibid.*
87 *Ibid.*
88 *Ibid.*
89 *Ibid.*
90 Study cybercrime questionnaire. Q19.

Sufficient jurisdiction?

Overall, analysis of provisions in international and regional instruments, and the law and practice of states, suggests that cybercrime jurisdictional challenges can be resolved by ensuring clarity, and innovative application, of existing principles.

As highlighted by commentators, *'transactions in cyberspace involve real people in one territorial jurisdiction either (i) transacting with real people in other territorial jurisdictions or (ii) engaging in activity in one jurisdiction that causes real-world effects in another territorial jurisdiction.'*[91] As a result, forms of territoriality and nationality-based jurisdiction are almost always able to ensure that a 'sufficient connection' or 'genuine link' can be established between cybercrime acts and at least one state. This Study does not therefore find that there is a need, at present, for additional jurisdiction over a 'cyberspace' dimension. The vast majority of cybercrime acts fall within the two categories above and can be genuinely linked to particular states. As such – and as discussed later in this Chapter – the fact that data are increasingly transient and dispersed through global data centres, currently presents a challenge more for the collection of *evidence*, than it is does for establishment of *jurisdiction*. To the extent that the *elements* and *effects* of an individual cybercrime act could *all* be transient and dispersed, forms of jurisdiction may still rely on nationality-based principles and (for legal persons), place of incorporation principles.

As discussed in Chapter Four (Criminalization) in the context of international human rights law, however, one risk of the projection of extensive extra-territorial jurisdiction may be to the plurality of internet content. At the heart of the jurisdictional debate, lies interpretation of the placement of offence elements and effects within geographical boundaries. Whether this is viewed from the perspective of 'acts,' 'conduct,' 'circumstances,' 'data,' or 'computer systems,' the avoidance of jurisdictional conflicts must depend upon the maintenance of a sufficiently high threshold for the 'genuine link' – together with clear inter-state communication channels for coordination of extra-territorial criminal justice actions.

[91] Post, D.G., 2002. Against 'Against Cyberanarchy.' *Berkeley Technology Law Journal* (17):1365-1387.

7.3 International cooperation I – formal cooperation

Key results:

- Due to the volatile nature of electronic evidence, international cooperation in cybercrime matters requires timely response and the ability to request specialized investigative actions
- Use of traditional forms of international cooperation predominates for obtaining extra-territorial evidence in cybercrime cases. Over 70 per cent of responding countries reported using formal mutual legal assistance requests for this purpose
- Within such formal cooperation, almost 60 per cent of requests use bilateral instruments as the legal basis. Multilateral instruments are used in around 20 per cent of cases
- Response times for formal mechanisms are reported to be of the order of months, for both extradition and mutual legal assistance requests
- Urgent channels for mutual legal assistance requests do exist in some countries, however the impact of these on response times is unclear
- The current international cooperation picture risks the emergence of country clusters that have the necessary powers and procedures to cooperate amongst themselves, but are restricted, for all other countries, to 'traditional' modes of international cooperation that may take no account of the specificities of electronic evidence

This section examines mechanisms of international cooperation in cybercrime matters found in international instruments, and in national law and practice.

Cooperation provisions in international and regional instruments

As discussed in Chapter Three (Legislation and frameworks) of this Study, a number of international and regional cybercrime instruments contain international cooperation provisions. Instruments typically either contain broad general obligations on States parties to cooperate,[92] and/or particular cooperation mechanisms, including extradition[93] and mutual legal assistance.[94] The table below summarizes international cooperation provisions in key binding and non-binding international and regional cybercrime instruments. Further details and article numbers are also included in the table at Annex Three to this Study.

92 Commonwealth of Independent States Agreement, Art. 5; Council of Europe Cybercrime Convention, Art. 23; Shanghai Cooperation Organization Agreement, Art. 3-5. The Draft African Union Convention refers to the principle in Art. III(14).

93 COMESA Draft Model Bill, Art. 42(c); Council of Europe Child Protection Convention, Art. 38(3); EU Decision on Fraud and Counterfeiting, Art. 10.

94 Commonwealth of Independent States Agreement, Art. 6; Council of Europe Child Protection Convention, Arts. 25, 27; ECOWAS Draft Directive, Art. 35; League of Arab States Convention, Arts. 32, 34.

Cooperation provisions in international and regional cybercrime instruments								
	Binding instruments					Non-binding instruments		
International cooperation provisions	**Draft African Union Convention**	**Commonwealth of Independent States Agreement**	**Council of Europe Cybercrime Convention**	**League of Arab States Convention**	**Shanghai Cooperation Organization Agreement**	**COMESA Draft Model Bill**	**Commonwealth Model Law**	**ITU/CARICOM/ CTU Model Legislative Texts**
General international cooperation								
General principle of international cooperation	■	■	■	–	■	■	–	–
Extradition for instrument offences	–	–	■	■	–	■	–	–
General mutual legal assistance	–	■	■	■	–	■	–	–
Specific assistance								
Expedited assistance	–	■	■	■	–	■	–	–
Preservation of computer data	–	–	■	■	–	■	–	–
Seizure/access to/collection of/disclosure of computer data	–	–	■	■	–	■	–	–
Other forms of cooperation								
Trans-border access	–	–	■	■	–	■	–	–
24/7 network	–	–	■	■	–	■	–	–
Additional provisions								
Dual criminality requirements	–	–	■	■	–	■	–	–

A key starting point in examining such provisions is the *scope* of the *cooperation*. Whereas *jurisdiction* provisions in international and regional instruments usually refer to the particular offences established under the instrument, *international cooperation* provisions may either 'bite' on the offences themselves and/or have a wider scope.

Examination of the five binding instruments shows that international cooperation provisions in all instruments have a scope related to 'cybercrime' or closely-related concepts, such as 'offences relating to computer information' or 'information and information technology offences.' In addition, two instruments (the Council of Europe Cybercrime Convention and the League of Arab States Convention) extend mutual legal assistance provisions to the gathering of electronic evidence in *any* offence. As noted in Chapter Six (Electronic evidence and criminal justice), this is important in the context of an increasing role for electronic evidence in the investigation and prosecution of all forms of crime. The implications of such variation in international cooperation scope are considered in this Chapter.

Instrument	Scope of international cooperation provisions
Draft African Union Convention	• 'Cybercrime'
Commonwealth of Independent States Agreement	• 'Offences relating to computer information'
Council of Europe Cybercrime Convention	• 'Criminal offences related to computer systems and data' • 'Collection of evidence in electronic form of a criminal offence'
League of Arab States Convention	• 'Information and information technology offences' • 'Gathering of electronic evidence in offences'
Shanghai Cooperation Organization Agreement	• 'International information security'

Cooperation mechanisms contained within international and regional cybercrime instruments must also be placed in the wider international cooperation context. While a number of the instruments can be relied upon as a legal basis for specific cooperation acts,[95] it must be remembered that States parties to the instruments are also party to broader networks of multilateral and bilateral agreements relating to cooperation in criminal matters – including treaties such as the Organized Crime Convention. Depending upon the nature of the act under investigation, it is possible that cooperation needs can fall within a range of legal mechanisms. Some of the cybercrime instruments recognize this point. The Council of Europe Cybercrime Convention for example provides that parties shall co-operate with each other, not only '*in accordance with the provisions of this chapter*' but also '*through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws.*'[96]

Finally, it is important to emphasize that *non*-binding instruments cannot provide the same international legal basis for cooperation as binding instruments. While the COMESA Draft Model Bill, for example, specifies that '*the legal authorities of* [*this country*] *shall cooperate directly and to the widest extent possible with legal authorities of another country,*'[97] this constitutes only a recommended provision to be included in national law. Even where such a provision is incorporated, countries generally still require a politico-legal *mechanism* for specific acts of cooperation – whether a multilateral or bilateral treaty, or an understanding of reciprocity – with the particular requesting country. In this respect, however, the existence in some countries of 'open-door' cooperation policies, under which national law enables cooperation, in principle, with any country, should also be noted.[98]

Extradition and mutual legal assistance in international and regional instruments

Two binding instruments included in the table above (the Council of Europe Cybercrime Convention and the League of Arab States Convention), and one non-binding instrument (the COMESA Draft Model Bill), specifically envisage extradition for offences contained therein.[99] All of these make extradition dependent upon dual criminality and seriousness of the offence. Three binding instruments (the Commonwealth of Independent States Agreement, the Council of Europe

95 See, for example, Council of Europe Cybercrime Convention, Arts. 24 et. seq.; League of Arab States Convention, Arts. 31 et seq.; Commonwealth of Independent States Agreement, Arts. 6 et seq.; COMESA Draft Model Bill, Arts. 42 et seq.

96 Council of Europe Cybercrime Convention, Art. 24.

97 COMESA Draft Model Bill, Art.41.

98 A few responding countries noted the existence of such policies (Study cybercrime questionnaire. Q220).

99 Council of Europe Cybercrime Convention, Art. 24; League of Arab States Convention, Art. 31; COMESA Draft Model Bill, Art. 42(c).

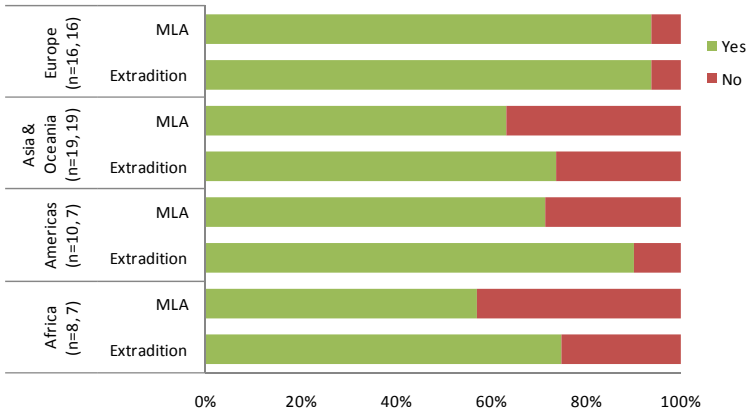
Cybercrime Convention, and the League of Arab States Convention) as well as the COMESA Draft Model Bill, also provide for general mutual legal assistance.[100] Some instruments envisage that mutual legal assistance requests may be subject to dual criminality.[101] Instruments also specify that requests may be refused where execution is considered 'contrary to national legislation,'[102] 'the request concerns a political offence,'[103] or the request is 'likely to prejudice sovereignty, security, *ordre public* or other essential interests.'[104]

Instruments further provide for expedited means of communication, such as email and fax, for requests in urgent matters,[105] with some requiring a 'reasonable' degree of security for such communications, and a written follow-up request within a certain period of time.[106] Finally, the Council of Europe Cybercrime Convention and the League of Arab States Convention include specific provisions on mutual legal assistance requests for: (i) expedited preservation of stored computer data; (ii) expedited disclosure of preserved traffic data; (iii) mutual assistance in the real-time collection of traffic data; and (iv) mutual assistance regarding the interception of content data.[107] Under the broad scope of the international cooperation provisions of these instruments, such specialized forms of assistance apply not only to computer-related crimes, but also to crimes in general.[108]

Use of cooperation mechanisms in cybercrime cases

At the level of national legislation, more than two thirds of countries in Africa, Asia and Oceania, and the Americas reported the existence of national legislation applicable to cybercrime extradition and mutual legal assistance matters. Almost all countries in Europe reported that such legislation exists. Legislation is typically more often in place for extradition than for mutual legal assistance.[109] Analysis of legislation cited by countries indicates that the vast majority of such laws are not cyber-specific, but rather cover extradition and mutual legal assistance in general criminal matters.[110] It should be noted that the absence of national legislation on extradition or mutual legal assistance does not necessarily prevent countries from engaging in international cooperation in cybercrime matters. International

Figure 7.3: Existence of legislation for extradition and MLA in cybercrime cases



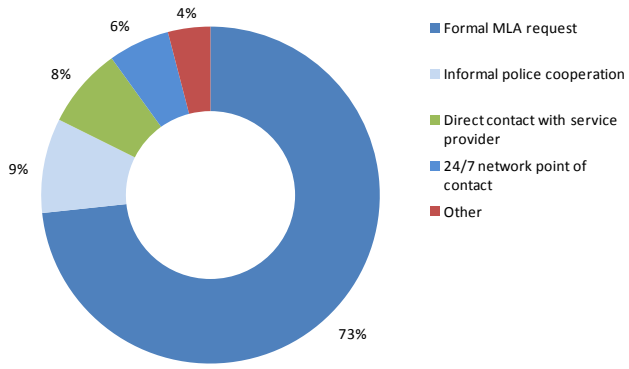
Source: Study cybercrime questionnaire. Q193 and Q216. (n=53, 49)

100 Commonwealth of Independent States Agreement, Art. 6; Council of Europe Cybercrime Convention, Arts. 25, 27; League of Arab States Convention, Arts. 32, 34; COMESA Draft Model Bill, Arts. 43(a), 45.
101 Council of Europe Cybercrime Convention, Arts. 24(1), 25(5); League of Arab States Convention, Arts. 32(5), 37(3) and (4); COMESA Draft Model Bill, Arts. 42(a), 43(d).
102 See, for example, COMESA Draft Model Bill, Art. 45(c)(i).
103 See, for example, League of Arab States Convention, Art. 35.
104 See, for example, Council of Europe Cybercrime Convention, Art. 27(4)(b).
105 Council of Europe Cybercrime Convention, Art.25(3); League of Arab States Convention, Art. 32(3).
106 Commonwealth of Independent States Agreement, Art. 6(2).
107 Council of Europe Cybercrime Convention, Arts. 29-31, 34; League of Arab States Convention, Arts. 37-39, 41, 42.
108 Although note that for real-time collection of traffic data and interception of content data, assistance must only be provided to the extent allowed by domestic law.
109 Study cybercrime questionnaire. Q193 and Q216.
110 *Ibid.*

cooperation matters may, for example, be handled under national mechanisms such as executive orders, or administrative policies.

The use of *formal* cooperation mechanisms in transnational cybercrime cases is predominant over other forms of cooperation. Figure 7.4 shows that over 70 per cent of law enforcement authorities reported that formal mutual legal assistance was most often used to obtain a range of evidence types from other jurisdictions.[111] Less-used mechanisms were reported to include informal police cooperation, direct contact with a service provider, and the use of 24/7 contact points.[112]

Figure 7.4: Means of obtaining extra-territorial evidence

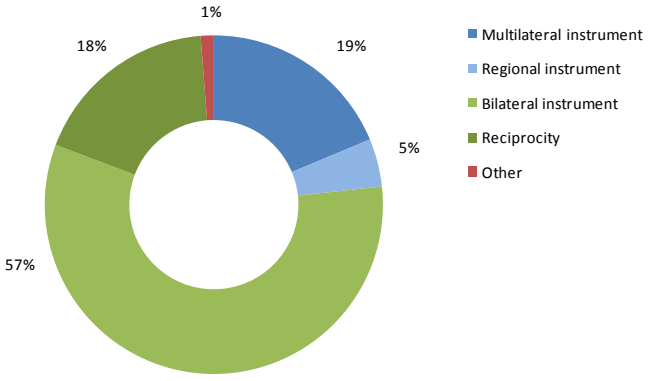


Source: Study cybercrime questionnaire. Q105. (n=56, r=221)

Within such formal cooperation, the use of *bilateral* instruments for cybercrime cases is most common. Almost 60 per cent of countries reported that they rely on bilateral instruments as the legal basis for extradition and mutual legal assistance in cybercrime cases.[113] A further 20 per cent cited reciprocity as the basis. Despite the fact that around 60 per cent of countries that responded to the Study questionnaire have signed or ratified an international or regional cybercrime agreement containing cooperation provisions,[114] only in 25 per cent of cases were international and regional instruments cited as the legal basis.[115]

The number of countries that responded to the question on the legal basis for cooperation is comparatively low. Results should therefore be interpreted with caution. Nonetheless, the predominant use of bilateral instruments and reciprocity reflects both: (i) the fact that not all countries are party to multilateral instruments; and (ii) use of 'traditional' modes of international cooperation, even where countries are party to multilateral instruments. In this respect, no country reported the existence of cyber-specific bilateral instruments, and none were identified in the course of research for the Study.

Figure 7.5: Legal basis of cybercrime extradition and MLA requests



Source: Study cybercrime questionnaire. Q202-207 and Q227-232. (n=21, r=50)

111 Study cybercrime questionnaire. Q105.

112 *Ibid.*

113 Study cybercrime questionnaire. Q202-207 and Q227-232. The proportion of countries responding to these particular questions that had signed or ratified an international or regional cybercrime instrument was the same as for all responding countries.

114 Signatories or States Parties to the Council of Europe Cybercrime Convention (40 per cent), the League of Arab States Convention (10 per cent), the Commonwealth of Independent States Agreement (15 per cent), and the Shanghai Cooperation Organization Agreement (10 per cent). Numbers sum to more than 60 per cent due to multiple instrument membership for some countries.

115 Study cybercrime questionnaire. Q202-207 and Q227-Q232.

The use of 'traditional' modes of cooperation may not present difficulties when used between countries that are *also* parties to multilateral instruments. Countries will likely be able to request specialized cybercrime investigative measures – such as preservation of computer data – as both parties will have the relevant procedural powers in national law. Use of 'traditional' modes where at least one country is *not* also party to a multilateral instrument, however, may present challenges. This is the case for the majority of countries in the world. Globally, over 60 per cent of countries are not party to any multilateral cybercrime instrument – with the result that they have no *international* legal obligation to either include specialized cybercrime investigative powers in national procedural laws, or to carry out specialized investigations in response to cooperation requests.[116]

Some 20 per cent of responding countries reported, for example, that national legislation does not provide for expedited preservation of computer data.[117] As might be expected, the majority (80 per cent) of these countries have not signed or ratified any of the binding international or regional cybercrime instruments. Presently, requests for international cooperation to such countries must be made by 'traditional' bilateral and reciprocity-based means. However, if actions such as expedited preservation of data are requested, the request may suffer from: (i) a lack of clarity concerning whether such measures can be requested under the relevant bilateral instrument or arrangement, and/or (ii) the non-existence of such measures under national criminal procedure law.

Dual criminality and other conditions in cybercrime cooperation

Use of international cooperation for the investigation of cybercrime acts can also create challenges regarding the equivalence of criminalization. Cooperation requests are commonly subject to a range of both procedural and substantive requirements – in respect of which the requested state must be satisfied before consent can be granted. One key requirement is that of *dual criminality*. The principle of dual criminality requires that the act to which a request relates be a crime according to the criminal law of the request*ed* state, as well as the request*ing* state.[118] Dual criminality features in international and regional cybercrime instruments. It is required for extradition, and envisaged for forms of mutual legal assistance, for example, under the Council of Europe Cybercrime Convention and the League of Arab States Convention.[119]

A key factor in establishing dual criminality is the substantive underlying conduct, and not the technical terms or definitions of the crime in national laws.[120] The Council of Europe Cybercrime Convention clarifies that dual criminality shall be deemed fulfilled '*irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party*' if '*the conduct underlying the offence*' for which assistance is sought '*is a criminal offence under its laws*.'[121] According to this approach, the focus is on 'transposing' the elements of the act into the law of the request*ed* state in order to confirm that the act would also be a criminal offence.[122]

---

116 Although, as noted in Chapter Five (Law enforcement and investigations), they may well make use of existing general investigative powers.

117 Study cybercrime questionnaire. Q49.

118 UNODC, 2012. *Manual on Mutual Legal Assistance and Extradition*. Dual or double criminality is not so much a rule of customary international law as a treaty and statute consideration based on policy and expediency (Williams, S.A., 1991. The Double Criminality Rule and Extradition: A Comparative Analysis. *Nova Law review*, 15:582).

119 References to the concept can be found in Council of Europe Cybercrime Convention, Arts. 24(1), 25(5), 29(3) and (4); League of Arab States Convention, Arts. 32(5), 37(3) and (4).

120 Article 43(2) of the United Nations Convention against Corruption, for example, states that '*In matters of international cooperation, whenever dual criminality is considered a requirement, it shall be deemed fulfilled irrespective of whether the laws of the requested State Party place the offence within the same category of offence or denominate the offence by the same terminology as the requesting State Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under the laws of both States Parties*.'

121 Council of Europe Cybercrime Convention, Art. 25(5).

122 Two approaches exist in this respect: Dual criminality *in abstracto* and dual criminality *in concreto*. '*In abstracto*' means that consideration of the behaviour in question is limited to the question of whether the behaviour is punishable, regardless of its legal qualification or the existence of possible reasons excluding punishability. '*In concreto*' means that the behaviour fulfils all

Some cybercrime acts may be clearly criminalized in one country and not in another – hence failing the dual criminality test. The production, distribution or possession of computer misuse tools, for example, is not criminalized in almost 20 per cent of countries that responded to the Study questionnaire.[123] Requests related to this crime directed to these countries will clearly suffer from dual criminality challenges.

For acts that *are* broadly criminalized across countries – such as computer-related acts causing personal harm – many of the nuanced differences in legislation discussed in Chapter Four (Criminalization) will not present a bar to the establishment of dual criminality. Nonetheless, depending upon the approach taken by national authorities in cooperation proceedings – such as extradition hearings – differences in the criminalization of particular cybercrime acts can become relevant. In some countries, aspects such as the 'use of technical means' to commit an offence (in the case of illegal interception), or 'thresholds' of insult (in the case of content offences), can be considered to be *constituent elements* of the crime – meaning that there is no crime unless they are present. In such circumstances, challenges to dual criminalization may legitimately arise. One responding country referred to dual criminality challenges in the case of computer-related copyright offences and computer-related fraud, noting – as the requested country – that there was no equivalent crime to that which was the subject of the request.[124]

In addition, dual criminality can have a significant role to play in mutual legal assistance requests[125] – including where assistance measures concern the collection of electronic evidence for 'any offence' (rather than specific 'cybercrime' or 'computer-related' offences). The Council of Europe Cybercrime Convention, for example, allows that States parties can apply dual criminality requirements to requests for preservation of computer data.[126] As geographically-dispersed electronic evidence becomes increasingly central to 'conventional' crime investigations, the extent to which dual criminality is required will become a key consideration. On the one hand, a number of countries reported that they only require the existence of dual criminality when the measures requested are '*particularly intrusive,*' such as search and seizure,

Example of cyber-specific legislation on international cooperation passed by a country from Western Africa

Preservation and expedited disclosure of computer data within international cooperation

(1) [The State] may be requested to expedite preservation of data stored in a computer system located in [the State], referring to crimes described under this Act, pursuant to the submission of a request for assistance for search, seizure and disclosure of those data.
(2) …
(3) In executing the demand of a foreign authority under the preceding sections, the Attorney-General of the Federation may order any person who has the control or availability of such data, including a service provider, to preserve them.
(4) to (6) …
(7) A request for expedited preservation of computer data may be refused if there are reasonable grounds to believe that the execution of a request for legal assistance for subsequent search, seizure and release of such data shall be *denied for lack of verification of dual criminality.*

requirements of punishability, including the absence of any justification such as self-defence, excuse, or other reasons excluding punishability. (See Council of Europe European Committee on Crime Problems, 2012. *Note on dual criminality, in concreto or in abstracto.* PC-OC (2012) 02 Final, 11 May 2012.)

123 Study cybercrime questionnaire. Q28.

124 Study cybercrime questionnaire. Q215.

125 With respect to criminal cooperation in general, dual criminality for mutual legal assistance can range from not being required at all, to being required for certain coercive acts of mutual legal assistance, to being required for any type of mutual legal assistance. (See UNODC, 2012. *Manual on Mutual Legal Assistance and Extradition*).

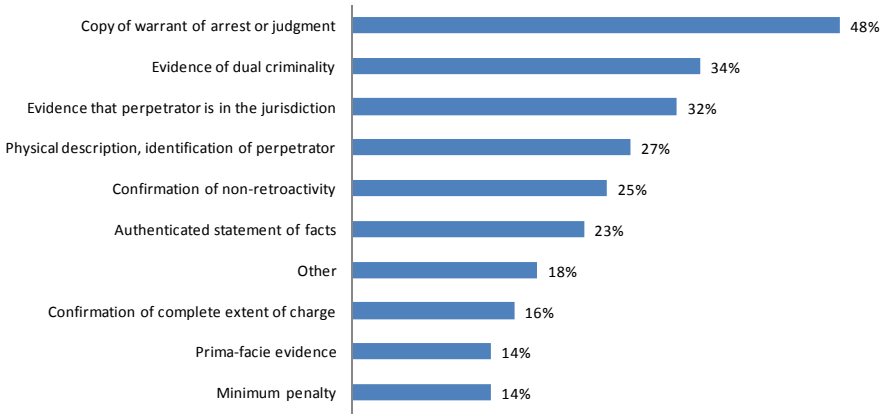
126 Council of Europe Cybercrime Convention, Art. 28(4). Note that mutual legal assistance requests under the Convention apply to criminal offences related to computer and data, as well as to the collection of evidence in electronic form of any criminal offence.

wiretapping or surveillance.[127] On the other hand, dual criminality has an important role to play in the protection of a state's sovereignty over its own law enforcement and criminal justice affairs. Dual criminality protection could, for example, provide a legal basis for countries to refuse requests for supply of electronic evidence concerning internet content-related offences that are not criminalized in the requested country. In cases involving mutual legal assistance and internet content, in particular, additional bases for refusal such as political offence exceptions, state essential interest exceptions,[128] and even international human rights obligations may be invoked.[129] Indeed, when asked about common reasons for rejection of cybercrime mutual legal assistance requests, '*breach of human rights obligations*' was specifically highlighted by responding countries.[130]

Finally, in addition to the question of the *existence* of a criminal offence in the law of the requested state, many multilateral and bilateral instruments also establish *seriousness* thresholds for international cooperation requests.[131] Thresholds are included, for example, in the Council of Europe Cybercrime Convention and League of Arab States Convention – both of which provide for extradition for offences established in accordance with the Convention '*punishable under the laws of both Parties*' (dual criminality requirement) by '*deprivation of liberty… of at least one year, or by a more severe penalty*' (threshold standard).[132] During information gathering for the Study, countries reported that cybercrime acts are widely considered to meet seriousness standards – thereby constituting extraditable offences. All responding countries in Europe and the Americas, and 90 per cent of countries in Africa, Asia and Oceania reported that cybercrime acts are, in general, extraditable offences.[133]

The constraint of dual criminality was highlighted by countries when asked about 'pre-conditions' for cybercrime cooperation requests. Such conditions can be considered to have both a procedural and a substantive nature, and the way in which different conditions are considered may vary between countries.[134] While countries reported both procedural and substantive elements, dual criminality was nonetheless identified as a requirement for

Figure 7.6: Pre-conditions before extradition request in cybercrime cases can be considered



Source: Study cybercrime questionnaire. Q198. (n=44, r=110)

127 Study cybercrime questionnaire. Q198.
128 See, for example, Council of Europe Cybercrime Convention, Art. 29(4).
129 See, for example, Currie, R.J., 2000. Human Rights and International Mutual Legal Assistance: Resolving the Tension. *Criminal Law Forum*, 11(2):143-181.
130 Study cybercrime questionnaire. Q239.
131 See, for example, Organized Crime Convention, Arts. 2, 3, and 16.
132 Council of Europe Cybercrime Convention, Art. 24.
133 Study cybercrime questionnaire. Q194.
134 For extradition, a copy of the arrest warrant and physical description of the suspect may, for example, be considered as procedural elements subject to an initial 'regularity' check. The existence of dual criminality, on the hand, may be considered in depth at an extradition hearing before a judicial authority (Response from regional expert nominated by WEOG to preliminary results from the Study).

both extradition and mutual legal assistance.[135] In the case of extradition, countries also frequently identified expected procedural requirements such as a copy of the arrest warrant or judgement, and evidence that the suspect was in the jurisdiction.[136] In the case of mutual legal assistance, countries identified conditions such as assurances regarding the sufficiency of evidence requested, and an authenticated statement of facts.[137]

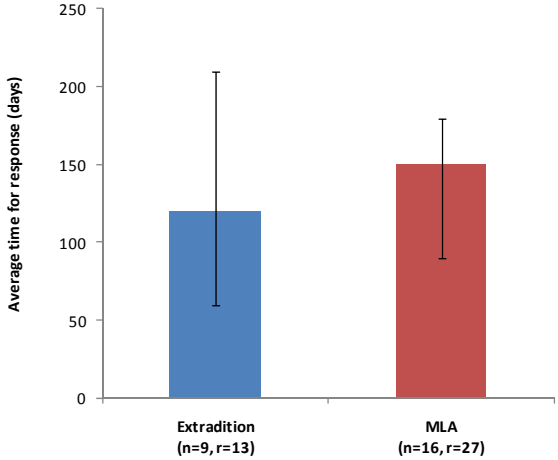
While a number of countries indicated that they had not rejected any cybercrime extradition or assistance request to date, a failure to satisfy both procedural and substantive requirements was emphasized by countries when asked about common reasons for rejection of requests.[138] Countries most commonly reported procedural irregularities and insufficient provision of evidence – highlighting the need for the careful preparation of cooperation requests.[139] Substantive reasons provided concerned dual criminality, and international human rights law obligations.[140] Notably, one country reported the practical problem of '*volatility of computer data*' as a reason for refusing mutual legal assistance requests[141] – perhaps indicating that requests could not be fulfilled as relevant electronic evidence had already been deleted. This relates closely to the time needed for response to formal modes of cooperation – an issue addressed below.

Extradition and mutual legal assistance in practice

Available statistics reported through the Study questionnaire show that extradition and mutual legal assistance are used to varying extents by countries. Around half of responding countries reported fewer than 10 cybercrime extradition or mutual legal assistance cases sent or received per year.[142] The average number of cases was 8 per year, with three-quarters of all reported cases falling within the range of 3 to 45 cases per year. Countries with the highest numbers of cases were typically larger countries in Europe or North America.

The distribution of cybercrime offences that are the subject of extradition and mutual legal assistance requests is largely similar to the total caseload handled by law enforcement in general – constituting around one-third each of acts against the confidentiality, integrity and availability of computer systems or data, acts for personal or financial gain or harm, and content-related acts.[143] Measures most commonly reported to be available to requesting states for the investigation of these acts include provision of stored content or traffic data, or search and seizure of computer hardware or data.[144] In line with the fact that some

Figure 7.7: Average response time (days) for cybercrime extradition and MLA requests



Source: Study cybercrime questionnaire. Q213 and Q238.

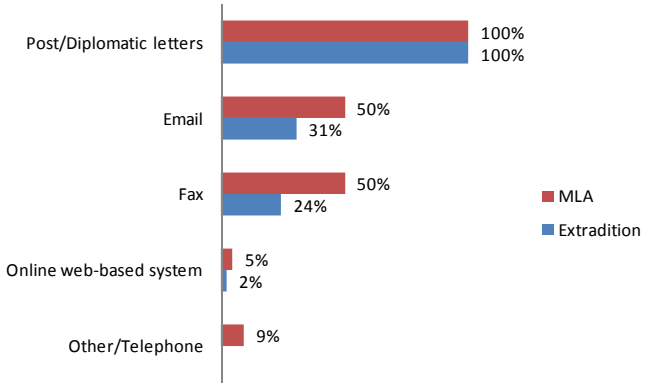
135 Study cybercrime questionnaire. Q198 and Q220.
136 *Ibid.* (Q198).
137 *Ibid.* (Q220).
138 Study cybercrime questionnaire. Q214 and Q239.
139 *Ibid.*
140 *Ibid.* (Q239).
141 *Ibid.* (Q239).
142 Study cybercrime questionnaire. Q202-206 and Q227-231.
143 Study cybercrime questionnaire. Q208-211 and Q233-236.
144 Study cybercrime questionnaire. Q221.

countries do not have specialized investigative powers, such as preservation of computer data or real-time collection of content or traffic data in national laws, only around 35 per cent and 45 per cent of countries, respectively, reported that such actions could be requested through mutual legal assistance.[145]

While the range of offences covered and investigative powers available through formal international cooperation is expansive, the mechanism is challenged by long response times in practice. Countries reported median response times of 120 days for extradition requests, and 150 days for mutual legal assistance requests, received and sent.[146] The data should be considered with some caution, due to the comparatively low number of countries that responded to the question, and due to the possibility that countries applied a range of timescale definitions in responding to the question – for example, from 'request receipt' to 'initial response', or from 'request receipt' to 'substantive resolution'. Given the fact that 75 per cent of all responses times reported fall within the 'error bar' lines,[147] however, it is clear that the use of formal cooperation mechanisms occurs on a timescale of months, rather than days.

Long time scales in international cooperation may be related to reliance on 'traditional' formal channels of communication that typically necessitate the involvement of multiple authorities in the communication chain. All countries, for example, reported using post or diplomatic letters for both extradition and mutual assistance requests in cybercrime cases.[148] A number of countries highlighted that the manner of transmission of requests is governed by the provisions of the relevant bilateral treaty or multilateral convention. In some cases, these include the requirement for formal modes of communication.[149]

Figure 7.8: Forms of communication in cybercrime cases



Source: Study cybercrime questionnaire. Q197 and Q219. (n=44,47, r=77,94)

Mechanisms of formal cooperation usually require the designation of 'central authorities' – and it is these authorities that typically handle incoming and outgoing requests by post or diplomatic letters. The Commonwealth of Independent States Agreement, for example, requires States parties to establish '*a list of competent authorities.*'[150] The Council of Europe Cybercrime Convention requires parties to indicate central authorities for extradition and for mutual legal assistance.[151] Insofar as cybercrime cases are largely handled in the same way as other crime cases, countries reported typical institutions assigned to the role of central authority also for cybercrime cooperation matters.[152] These included Offices of the Attorney General or Prosecutor General, and Ministries of Justice.[153] Some countries noted that different authorities were assigned the role of central authority depending upon the stage

145 *Ibid.*
146 Study cybercrime questionnaire. Q213 and Q238.
147 Error bars on the figure represent upper and lower quartiles.
148 Study cybercrime questionnaire. Q197 and Q219.
149 *Ibid.*
150 Commonwealth of Independent States Agreement, Art 4.
151 Council of Europe Cybercrime Convention, Arts. 24 and 27. Competent authorities notified under these articles are listed at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/Res_internatcoop_authorities_en.asp
152 Study cybercrime questionnaire. Q195 and Q217.
153 *Ibid.*

of proceedings.[154] While the central authority is responsible for coordinating a request, the ultimate *decision* on a request often lies with a different national authority.[155] For countries in Europe, for example, authorization of requests is not handled uniformly – ranging from a decision by a lower domestic court, to a decision by the executive branch of government.[156] In the other regions, prosecutors or magistrates also play an important role. The (often necessary) interplay between a range of government institutions can, in some cases, contribute to the long timescales reported for responses to requests.

As highlighted in Chapter Five (Electronic evidence and criminal justice), electronic evidence is volatile and may exist only for short periods of time – in many cases, significantly shorter time periods than those reported by states above. A number of responding countries highlighted, for example, that: '*Formal international cooperation mechanisms such as Mutual Legal Assistance (MLA) can be time consuming and cause delay in the investigation and prosecution of cybercrime offenses.*'[157] National laws governing mutual legal assistance very rarely contain cyber-specific provisions that reflect this reality.[158] Nonetheless, some bilateral and multilateral instruments, as well as national laws, do sometimes allow for expedited forms of communication, such as email, fax, or online systems.[159] The Council of Europe Cybercrime Convention and League of Arab States Convention, for example, provide that '*in urgent circumstances*' parties may make requests for mutual assistance by expedited means of communication, including fax or email, with formal confirmation to follow.[160] Non-binding instruments also envisage use of '*the most efficient means, […] provided that appropriate levels of authentication and security are utilized and formal confirmation follows the request or response.*'[161]

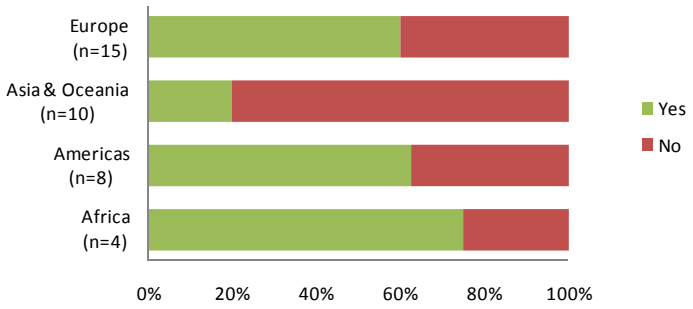
During information gathering for the Study, around half of responding countries reported the use of email or fax for mutual legal assistance requests. A much smaller proportion – 5 per cent – reported use of an online system. As might be expected given the role of mutual legal assistance in the investigation phase, the use of expedited forms of communication was greater for mutual legal assistance requests than for extradition requests.[162] In line with the requirements of international and regional cybercrime instruments, many countries noted that such communications were also followed-up by the use of post and diplomatic letters.[163] One country from South America stated that it used email and fax in order to monitor the extradition process, while Western Asian respondents pointed out that they only resorted to electronic communication in urgent cases.[164]

Roughly in line with levels of reported use of email, fax and telephone, over 60 per cent of countries in Africa, the Americas and Europe reported the existence of channels for urgent mutual legal assistance requests. Only 20 per cent of countries in Asia and Oceania, however, reported the existence of such channels. More than one third of respondents referred to specific urgent channel mechanisms, including INTERPOL national central bureaus, and G8 and Council of Europe 24/7 networks.[165] Being party to an international or regional instrument *envisaging* urgent mutual legal assistance channels appears to have a moderate effect – 55 per cent of responding countries that

154 *Ibid.*
155 Study cybercrime questionnaire. Q218.
156 *Ibid.*
157 Study cybercrime questionnaire. Q141.
158 Study cybercrime questionnaire. Q193 and Q216.
159 *Ibid.*
160 Council of Europe Cybercrime Convention, Art. 25(3), and League of Arab States Convention, Art. 32(3).
161 COMESA Draft Model Bill, Art. 43(b).
162 Study cybercrime questionnaire. Q197 and Q219.
163 *Ibid.*
164 Study cybercrime questionnaire. Q222.
165 *Ibid.*

were not party to any multilateral cybercrime instrument did not have channels for urgent requests, compared with 40 per cent of countries that were party to a multilateral cybercrime instrument.[166]

Figure 7.9: Channels for urgent MLA requests



Source: Study cybercrime questionnaire. Q222. (n=37)

The reported use of expedited means for cybercrime mutual legal assistance requests goes some way towards addressing challenges of electronic evidence volatility. However, only half of total responding countries reported use of such mechanisms. In addition, if overall formal assistance response times reported through the Study questionnaire *include* requests handled on an 'urgent' basis, then average response times – and indeed the predominate *distribution* of response times – is still measured in the order of months, as opposed to days. As discussed below, the situation is different in respect of *informal* modes of cooperation. While informal cooperation offers a more limited range of assistance, response times are typically faster.

7.4 International cooperation II – informal cooperation

Key results:

- Modes of informal cooperation are possible for around two-thirds of reporting countries, although few countries have a policy for the use of such mechanisms
- A number of informal cooperation networks in the area of cybercrime exist, including the G8 and Council of Europe '24/7' networks
- Initiatives for informal cooperation and for facilitating formal cooperation, such as 24/7 networks, offer important potential for faster response times, of the order of days
- Such initiatives may, however, be under-utilized. The number of cases handled by 24/7 networks reported by responding countries represented around 3 per cent of the total number of cybercrime cases encountered by law enforcement for that group of countries
- Analysis of formal and informal cooperation mechanisms is unable to find that the current global cooperation situation is sufficient. Globally, divergences in the scope of cooperation provisions in multilateral and bilateral instruments; a lack of response time obligation; multiple informal law enforcement networks; and variance in cooperation safeguards represent significant challenges to effective international cooperation regarding electronic evidence in criminal matters

International and regional perspectives

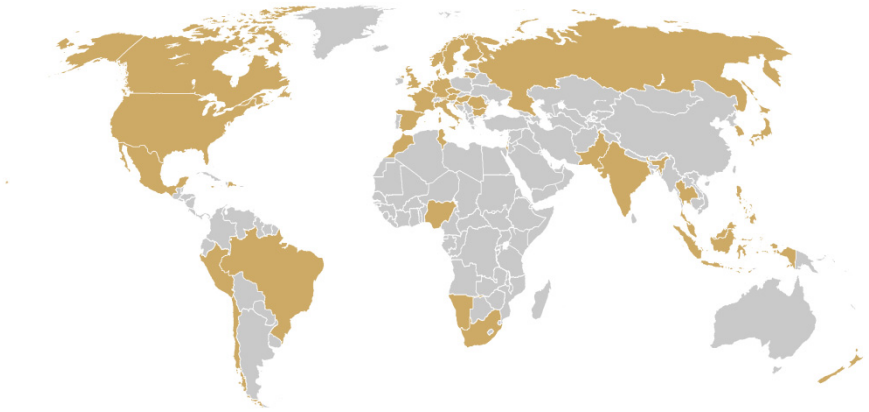
In addition to forms of formal international cooperation, steps in the process of extra-territorial law enforcement investigations may be undertaken by *informal* police-to-police or agency-to-agency communication. Such communication can be used *prior* to a formal mutual legal assistance

[166] *Ibid.*

request to a competent authority, or to *facilitate* a formal request.

Informal modes of cooperation are envisaged, in particular, by the Council of Europe Cybercrime Convention and the League of Arab States Convention. While informal cooperation can be mediated by direct police-to-police communication, or through international networks such as that of INTERPOL, both of these instruments require States parties to designate a 'specialized point of contact'. The contact point is charged with ensuring the provision of prompt assistance in criminal investigations related to computer systems and data or for the collection of evidence in electronic form of a criminal offence.[167] Under the Council of Europe Cybercrime Convention, '24/7' points of contact shall facilitate, or, if permitted by domestic law and practice, directly carry out: (i) provision of technical advice; (ii) preservation of data; and (iii) collection of evidence, provision of legal information, and locating of suspects.[168] More broadly, the Organized Crime Convention also requires States Parties to consider entering into arrangements on '*direct cooperation between their law enforcement agencies*'.[169]

Figure 7.10: Members of G8 24/7 network (2007)



Source: G8 24/7 Protocol Statement

Globally, a number of informal cybercrime cooperation networks exist. In addition to the 24/7 network of States parties to the Council of Europe Cybercrime Convention,[170] the G8 Subgroup on High-Tech Crime has established a 24/7 network in order to enhance and supplement traditional methods of obtaining assistance in cases involving networked communications and other related technologies.[171] As the map shows, membership of the G8 network includes countries that are party to a number of different international and regional instruments – offering opportunities for informal cooperation, and faster access to formal cooperation, amongst countries that may not otherwise be able to rely on shared multilateral legal cybercrime instruments.[172]

24/7 networks offer the practical advantage of a readily accessible, known starting point for cooperation requests. The evolution of multiple networks, however, may risk detracting from the 'single contact' strength of the system. During

> '**Informal cooperation** is used […] 80 per cent of the time, **because it is faster, particularly as an investigation unfolds**. There is **no time to waste** making formal requests, which will frustrate the investigation.'
>
> Source: Study cybercrime questionnaire. Q223 (response from a country in Western Africa).

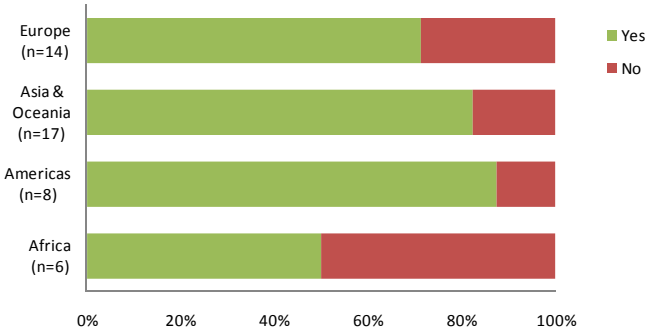
167 Council of Europe Cybercrime Convention, Art. 35; League of Arab States Convention, Art. 43.
168 *Ibid.* (Council of Europe Cybercrime Convention).
169 Organized Crime Convention, Art. 27(2).
170 Designated 24/7 points of contact under Council of Europe Cybercrime Convention, Art. 35, are available at: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Internationalcooperation/Res_internatcoop_authorities_en.asp
171 Council of Europe, 2008. *The Effectiveness of International Co-operation against Cybercrime: Examples of Good Practice*. p.13.
172 The G8 24/7 network membership as of December 2007. See http://www.oas.org/juridico/english/cyb_pry_G8_network.pdf

information gathering for the Study, for example, one country noted that the national contact point for the G8 network is located within a law enforcement institution, while the national contact point for the 24/7 network established under the Council of Europe Cybercrime Convention is located within a prosecution office attached to a superior court.[173] The presence of multiple contact points in a country can make it challenging for other countries to know which focal point to approach. It may also lead to delay in responding to requests when request*ed* countries need to verify the validity or identity of a focal point from a mechanism with which they have not previously communicated.

National approaches to informal cooperation

The majority of responding countries indicated that assistance can be provided informally, as well as through formal mutual legal assistance.[174] The proportion of countries able to provide informal assistance was notably higher in Europe, Asia and Oceania and the Americas (between 70 and 90 per cent) than in Africa (around 50 per cent).[175]

Figure 7.11: Can assistance be provided informally, as well as through a formal MLA request?



Source: Study cybercrime questionnaire. Q223. (n=45)

Countries that make use of informal cooperation noted that such mechanisms were dependent upon the existence of a competent and well-organized foreign counterpart. Countries observed that this was more likely when informal law enforcement cooperation was governed by some form of agreement. A number of countries reported that informal cooperation is therefore conducted on the basis of regional and bilateral agreements, through use of networks established by international and regional organizations and institutions; with the assistance of embassies and consulates; as well as through private networks among law enforcement officers.[176] While some countries referred to direct police-to-police cooperation, others spoke primarily of informal cooperation through INTERPOL channels.[177] One country noted that this was consistent with the realities of international legal cooperation, insofar as informal means of communication – however flexible and useful they might be – often only exist among states who have developed long-term working relationships.[178] Exchange of international case information through established international police channels is identified as a necessary step to the successful investigations.

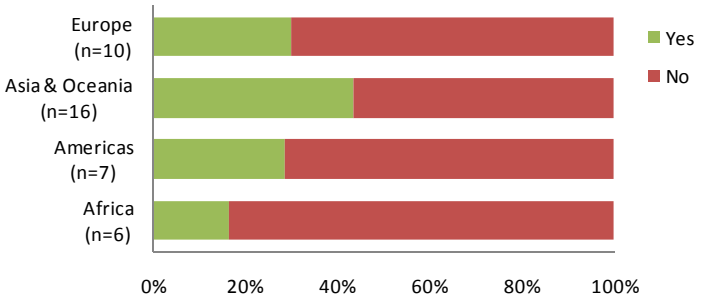
Even though informal modes of cooperation are likely more effective when based on a clear agreement, the majority of countries reported that the use of informal cooperation, rather than formal mutual legal assistance, was *not* subject to a defined policy.[179] A number of countries, however, did highlight the existence of guidelines and protocols, including 'unwritten' rules.

---

173 Response from regional expert nominated by WEOG to preliminary results from the Study.
174 Study cybercrime questionnaire. Q223.
175 *Ibid.*
176 *Ibid.*
177 Study cybercrime questionnaire. Q106 and Q223.
178 Response from regional expert nominated by Asian Group to preliminary results from the Study.
179 Study cybercrime questionnaire. Q224.

Where rules do exist, they were reported to be contained within national legislation, such as mutual assistance in criminal matters acts.[180] Practice varies, in particular, regarding who is designated to authorize informal assistance. Options given ranged from the local superintendent or senior investigating officer, to the head of the cybercrime division, to the case prosecutor or any judicial authority, to the Ministry of Justice.[181] The majority of countries tended to allow for decisions at the investigative level – by the local police or prosecutor, at times in concert with respective heads of agency.[182] One country from South-East Asia, for instance, noted that while the Office of the Attorney General is involved in formal requests, its involvement is not mandatory for assistance provided through informal cooperation channels.[183]

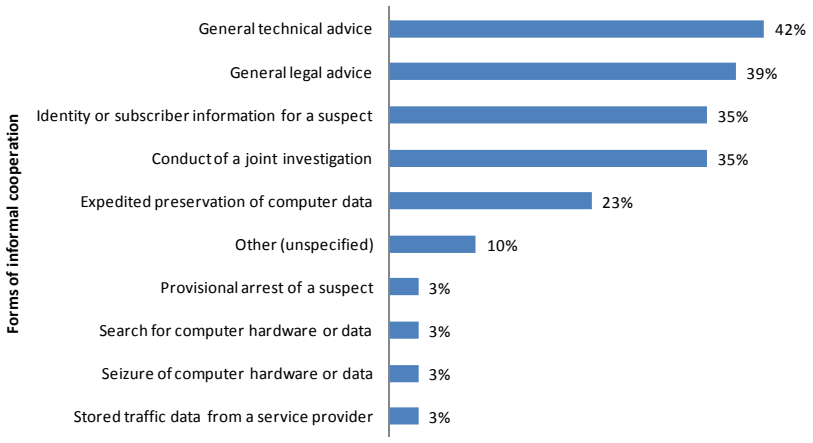
Figure 7.12: Policy for use of informal cooperation rather than MLA



Source: Study cybercrime questionnaire. Q 224. (n=39)

A general lack of policies did not, however, prevent countries from clearly indicating the types of assistance that can be provided through informal cooperation – albeit with some variation. Countries reported that general technical and legal advice is exchanged with counterparts in foreign law enforcement agencies almost on a daily basis. The majority of this information concerns joint investigations or general operational intelligence.[184] Almost all responding countries were able to provide such information informally, with only 10 per cent of countries stating that '*all informal requests are referred to the mutual legal assistance authority.*'[185] Some countries went further, and indicated that sharing of some personal data (including holders of telephone and post box numbers, information from hotel registers, and holders of IP addresses available without compulsory measures), obtaining public records such as criminal records, the taking of voluntary witness statements, and surveillance could be provided through direct law enforcement cooperation.[186]

Figure 7.13: Forms of informal cooperation with law enforcement agencies



Source: Study cybercrime questionnaire. Q106. (n=31, r=61)

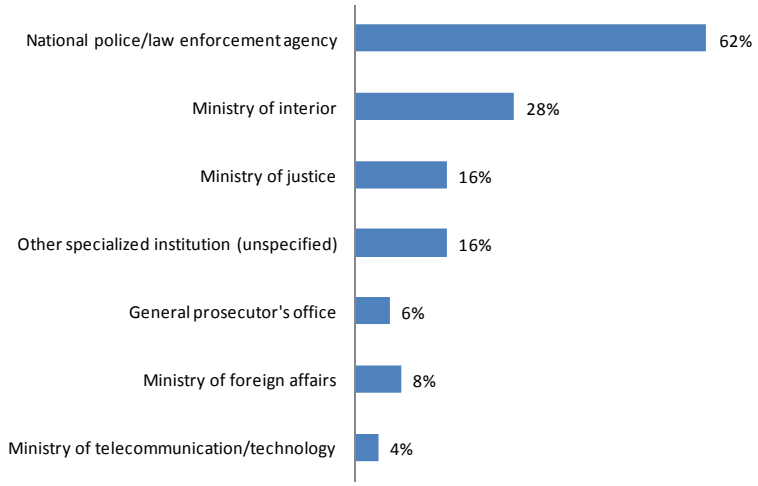
Generally, however, requests for specific investigative measures, such as expedited

180 *Ibid.*
181 Study cybercrime questionnaire. Q106, Q223 and Q224.
182 Study cybercrime questionnaire. Q106.
183 Study cybercrime questionnaire. Q223.
184 Study cybercrime questionnaire. Q106.
185 Study cybercrime questionnaire. Q223.
186 Study cybercrime questionnaire. Q106.

preservation of data, provisional arrest of a suspect, or search and seizure of hardware or data were stated to either require a formal mutual legal assistance request, or to be followed up a formal request within a short time period.[187] One country in Northern America, for example, stated that police to police cooperation '*does not allow for the use of compulsory evidence gathering orders, like the issuance of subpoenas or production orders, the execution of search warrants or other Criminal Code warrants.*'[188] Only one country indicated that all types of formal assistance were also available through informal means. The most usual situation (over two thirds of responding countries) was that that '*some assistance*' could be provided informally.[189] This fits with the finding that the majority of countries rely on *formal* means to obtain extra-territorial evidence in cybercrime investigations.[190]

24/7 Contact points – In line with initiatives at the international and regional level, such as the G8 24/7 network, over 70 per cent of all responding countries reported the existence of an institution serving as a 24/7 point of contact.[191] It is likely, however, that this proportion significantly overstates the degree to which 24/7 contact points exist globally – in light of the current reach of international and regional 24/7 networks and the comparatively low number of responding countries from regions such as Africa. Nonetheless, a number of responding countries highlighted the important of 24/7 networks. One country, for example, stated that '*It is imperative to have a central point (HQ office) for access to the 24/7 INTERPOL contact list as well as the G8 24/7 Emergency points of contact.*'[192]Most commonly, 24/7 contact points are established within national police and law enforcement agencies, followed by Ministries of Interior and Justice.[193] As noted above, 24/7 contact points can both facilitate and, if authorized, act directly, both in respect of informal and formal cooperation. Perhaps unexpectedly, the most common requests reported to be received by 24/7 contact points were for identity or subscriber information, followed by requests for expedited preservation of data and supply of stored traffic data.[194] This is in-line with the functions envisaged for 24/7 contact points by, for instance, the Council of Europe Cybercrime Convention.[195]

Figure 7.14: Institution serving as 24/7 focal point



Source: Study cybercrime questionnaire. Q107. (n=50, r=70)

187 Study cybercrime questionnaire. Q106 and Q223.
188 *Ibid.* (Q223).
189 *Ibid.* (Q223).
190 Study cybercrime questionnaire. Q105.
191 Study cybercrime questionnaire. Q107.
192 Study cybercrime questionnaire. Q99.
193 *Ibid.*
194 *Ibid.*
195 Council of Europe Cybercrime Convention, Art. 35.

As regards most common crime types, countries reported that requests for assistance most often concerned computer-related production, distribution or possession of child pornography, and, additionally, the solicitation and 'grooming' of children. This is followed by requests concerning computer-related fraud or forgery.[196] The proportion of cases involving child pornography seen by 24/7 focal points is somewhat higher than for all cybercrime offences handled by law enforcement in general.[197] This may reflect a higher degree of transnational dispersement of victims and offenders in this crime. In contrast, one country in South America mentioned that its 24/7 focal point most frequently deals with offences regarding attacks on government systems, defacement of websites, botnet attacks, and phishing.[198]

Example of cyber-specific legislation on 24/7 networks from a country in Western Africa

Designation of contact point for 24/7 Network

(1) In order to provide immediate assistance for the purpose of international cooperation under this Act, the National Security Adviser shall designate and maintain a contact point that shall be available twenty-four hours a day, seven days a week.

(2) This contact point can be contacted by other contact points in accordance with agreements, treaties or conventions to which [this State] is bound, or in pursuance of protocols of cooperation with international judicial or law enforcement agencies.

(3) The immediate assistance to be provided by the contact point shall include:

a) technical advice to other points of contact;

b) expeditious preservation of data in cases of urgency or danger in delay;

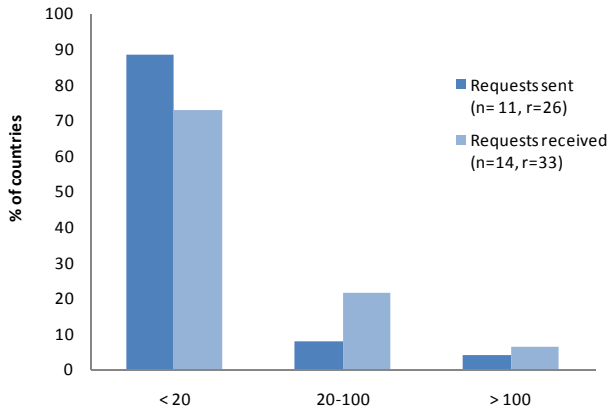
c) collection of evidence for which it has the legal jurisdiction in cases of urgency or danger in delay;

d) detection of suspects and providing of legal information in cases of urgency or danger in delay;

e) the immediate transmission of requests concerning the measures referred to in … this section, with a view to its expedited implementation.

Only a small number of countries (although with quite broad geographic distribution) were able to supply statistics regarding the *number* of requests sent and received by 24/7 contact points each year. Data reported through the Study questionnaire shows that more than 70 per cent of countries handled less than 20 requests (sent or received) through a 24/7 contact point per year. Only two responding countries handled more than 100 requests per year.[199]

Figure 7.15: Number of requests sent and received by focal point per year



Source: Study cybercrime questionnaire. Q107. (n=11,14, r=26,33)

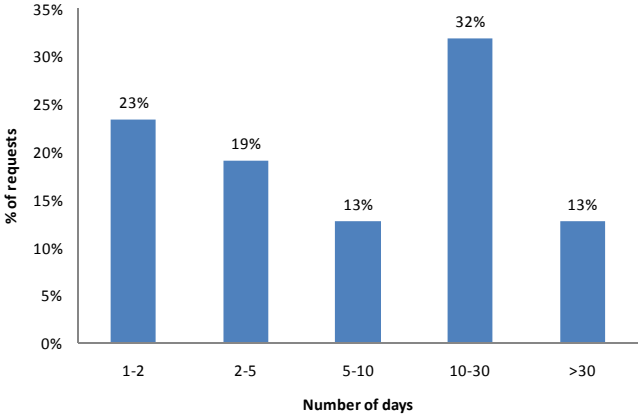
By way of comparison, law enforcement authorities in these same countries typically reported an average of almost 1,000 cybercrime cases per year.[200] Overall, for this group of countries, the *total* number of 24/7 requests reported per year, represents 3 per cent of the *total* number of cybercrime cases encountered by law enforcement per year.[201] By no means all cybercrime cases that come to the attention of law enforcement will require the involvement of a

196 Study cybercrime questionnaire. Q107.
197 See Chapter Two (The global picture), Section 2.2 The global cybercrime picture, Distribution of cybercrime acts.
198 Study cybercrime questionnaire. Q107.
199 *Ibid.*
200 Study cybercrime questionnaire. Q54-71.
201 Calculation based on Study cybercrime questionnaire. Q107 and Q54-71 for all countries that reported to both question sets.

24/7 network – many cases may be successfully investigated at the national level alone. Nonetheless, the group of countries that provided data on use of 24/7 contact points also stated that, on average, 60 per cent of cases involved a transnational dimension.[202] As such, there may be significant scope for more extensive use of the mechanism.

Underutilization of 24/7 networks risks losing potential gains in request response time. Countries responding to the Study questionnaire reported that almost 90 per cent of requests handled by 24/7 contact points received a response within one month.[203] Over 20 per cent of requests received a response within one to two days. A faster response time for 24/7 requests than for mutual legal assistance requests can be expected, not only due to the '24/7' nature of the system, but also due to the fact that – as a form of *informal* cooperation – the range of actions that can be carried out by a 24/7 contact point is more limited than that in *formal* mutual legal assistance.

Figure 7.16: Average time for response to requests sent and received by focal point for cooperation in cybercrime cases



Source: Study cybercrime questionnaire. Q107. (n=25, r=47)

As such, the 'response time' measured corresponds to a *different* set of assistance actions than those offered through mutual legal assistance – and the two 'response time' figures are not directly comparable. As discussed above, an informal mechanism, such as a 24/7 contact point, is more likely to provide general technical and legal advice and to *facilitate* more formal actions, than it is to undertake evidence gathering itself.[204] Nonetheless, the fact that 24/7 contact points often deliver a response within a matter of days represents an important opening of communication channels for the facilitation of more timely cooperation, including – potentially – actions that require a more formal request.

Sufficient cooperation?

This Chapter earlier found that current bases of jurisdiction likely *are* sufficient for avoiding jurisdictional gaps in the investigation and combating of cybercrime acts. The analysis of formal and informal cooperation mechanisms, on the other hand, is unable to find that the current global situation is sufficient for meeting cybercrime investigative and prosecutorial challenges.

While a number of options exist – including the use of informal cooperation, either directly or to facilitate formal cooperation – over 70 per cent of countries reported most often using formal mutual legal assistance requests to obtain electronic evidence located in another jurisdiction. Within formal mutual legal assistance, *bilateral* instruments dominate – drawing on traditional communication methods such as post and diplomatic letters and resulting in average response times of the order of months rather than days. As mentioned by countries, long cooperation response times create significant challenges due to the volatility of electronic evidence.

202 Study cybercrime questionnaire. Q83. Data only for countries that also responded to Q107.
203 Study cybercrime questionnaire. Q107.
204 See above, Section 7.4 International cooperation II – informal cooperation, National approaches to informal cooperation.

While many countries engage in *informal* cooperation in cybercrime cases on a faster time scale, the range of investigative actions that can be provided varies considerably, as well as the existence or not of clear policies on its use. Many countries acknowledge that evidence obtained through informal cooperation cannot be considered for sustainable supply of evidence at trial. Due perhaps to the diversity of approaches, informal cooperation might even be considered, in some cases, to be a cumbersome mechanism.[205] While '24/7' networks hold promise for streamlining informal cooperation and facilitating formal cooperation, they tend to be used comparatively infrequently when compared with the potential pool of transnational cybercrime cases that come to the attention of law enforcement authorities.

Many such challenges arise from differing membership of international and regional instruments. This can be seen in areas such as differences in the availability of urgent mutual legal assistance channels, and the ability to offer specialized measures, such as preservation of data, in response to cooperation requests. The current international cooperation picture risks the emergence of country clusters that have the necessary powers and procedures to cooperate amongst themselves, but are restricted, for all other countries, to 'traditional' modes of international cooperation that take no account of the specificities of electronic evidence. This is particularly the case for cooperation in investigative actions. A lack of common approach, including within current multilateral cybercrime instruments, means that requests for actions, such as expedited preservation of data outside of those countries with international obligations to ensure such a facility and to make it available upon request, may not be easily fulfilled. The inclusion of this power in the draft African Union Cybersecurity Convention may go some way towards closing this lacuna. Globally, divergences in the scope of cooperation provisions in multilateral and bilateral instruments; a lack of response time obligation; multiple informal law enforcement networks; and variance in cooperation safeguards, represent significant challenges to effective international cooperation regarding electronic evidence in criminal matters.

[205] Response from regional expert nominated by WEOG to preliminary results from the Study.

7.5 Extra-territorial evidence from clouds and service providers

Key results:

- Due to developments in cloud computing, data 'location,' while technically knowable, is becoming increasingly artificial, to the extent that traditional mutual legal assistance requests will often be addressed to the country that is the seat of the service provider, rather than the country where the data is physically located
- Through use of a live connection from a suspect's device, or through use of access credentials, investigators increasingly – knowingly or unknowingly – access extra-territorial data during evidence gathering, without the consent of the country where the data is physically situated
- Investigators may also occasionally obtain data from extra-territorial service providers through informal direct requests, although service providers more usually require due legal process
- Relevant existing provisions on 'trans-border' access found in the Council of Europe Cybercrime Convention and the League of Arab States Convention on Information Technology Offences do not adequately cover such situations – due to a focus on the 'consent' of the person having lawful authority to disclose the data, and presumed knowledge of the location of the data at the time of access or receipt
- Such challenges require: (i) (re)-conceptualization of the extent to which 'data location' can still be used as a guiding principle; and (ii) the development of common standards and safeguards concerning the circumstances, if any, under which direct access to extra-territorial data may be conducted by law enforcement

The challenge

As this Chapter has shown, current methods of international cooperation in cybercrime cases face significant challenges – including those of long response times for mutual legal assistance, and non-uniformity of national investigative powers for obtaining computer data as evidence. A third challenge – alluded to in the section on jurisdiction but not yet elaborated – is that of identifying the relevant jurisdiction to which a cooperation request for the obtaining of electronic evidence should be addressed in the first place. This challenge is becoming increasingly acute as computer services move to geographically distributed servers and data centres, collectively known as cloud computing.

Cloud computing services have been characterized as 'infrastructure-as-a-service,' 'software-as-a-service,' and 'platform-as-a-service,' covering the provision of 'virtual' machines over the internet, the provision of software applications, and the provision of a whole network, server system, operating system and storage, respectively.[206] In this sense, 'the cloud' is a new term for an old idea – harnessing another organization's infrastructure and expertise to deliver computing resources as a service over the internet. The physical hardware behind cloud services is housed in data centres located at strategic points designed to minimize delay in service delivery, as well as electricity and equipment-cooling costs. Users of Google services, for example, may access data

[206] See, for example, European Parliament Directorate General for Internal Polices, Citizens' Rights and Constitutional Affairs, 2012. *Fighting cybercrime and protecting privacy in the cloud.*

stored or processed in North America, South Eastern Asia, or Northern or Western Europe.[207]

It is frequently claimed that it cannot be known where in the cloud data is stored, and that data can be fragmented across multiple locations. It is certainly correct that databases can be hosted across multiple data centres, including in different countries, and containing multiple copies of the same data.[208] This may involve automated dynamic data placement across data centres physically located in different countries.[209] It is also true that contractual agreements between cloud service providers and users do not always divulge data centre location, or contain representations or conditions regarding the geographical location of where data will be held.[210] On the other hand, some cloud providers enable users to designate the physical region in which their data and servers will be located, and undertake not to move content from the selected region without notifying the customer.[211] In addition, geo-proof protocols are well under development for the remote identification of data source origin – enabling independent verification of the geo-location of data in the cloud.[212] Overall, increasing compliance requirements, customer demands, and data management technology are trending towards accurate cloud data location.

Nonetheless, it remains the case that – even when cloud data is geo-identified – it will reveal a pattern of dispersed, sometimes transient, data, including with copies in multiple jurisdictions. Where cloud data is evidence in a cybercrime investigation, it may well be 'extra-territorial' (in multiple countries) with respect to the investigating country. In many cases, however, even the basic fact of extra-territoriality may not be known for certain by law enforcement investigators.[213] Often, the starting point is merely the name of the cloud service provider – such as Amazon or Google. While the technical possibility may exist, it is extremely unlikely that a law enforcement investigator can know – at the outset of an investigation – in which country the cloud data is physically located (even given that it has not already been moved). If the investigating country is not the seat of the cloud service provider, a 'traditional' mutual legal assistance approach would require a communication to the central authority of the cloud provider's home jurisdiction, with a request for preservation and/or production of the computer data.

It is notable that under this approach, the mutual legal assistance request may not even be sent to the county *in which the data actually resides*. Facebook, for example, hosts the data of many users in a data centre in one country in Northern Europe,[214] but specifies that it discloses records in accordance with applicable laws cited from a country in North America.[215] For foreign law enforcement, Facebook guidelines indicate that a mutual legal assistance request or letter rogatory directed to the country in North America may be required to compel the disclosure of the contents

---

207 See http://www.google.com/about/datacenters/inside/locations/index.html

208 See, for example, http://www.datastax.com/wp-content/uploads/2012/09/WP-DataStax-MultiDC.pdf , referring to use of multi-data centre operations control across 'multiple geo-zones' by, amongst others, eBay and Netflix.

209 See, for example, Peterson, Z.N.J., Gondree, M., Beverly, R., 2011. *A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud*. For an example of automated data placement technology across geo-distributed data centres, see Agarwal, S., *et al.,* 2010. *Volley: Automated Data Placement for Geo-Distributed Cloud Services*.

210 Benson, K., Dowsley, R., Shacham, H., 2011. Do you know where your cloud files are? *Proceedings of the 3rd ACM Workshop on Cloud Computing Security*, pp.73-82.

211 See, for example, Amazon Web Services, 2012. *Risk and Compliance. November 2012*. Available at: http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf

212 *Ibid.* Demonstrating successful identification of approximate geolocations of data in Amazon's cloud. See also, Albeshri, A., Boyd, C. and Gonzalez Nieto, J., 2012. Geoproof: proofs of geographic location for cloud computing environment. *Proceedings of the 32nd International Conference on Distributed Computing Systems Workshops 2012*, IEEE, Macau, China, pp.506-514.

213 Although it may, perhaps, be assumed based on a broad knowledge of cloud service provider data centre locations.

214 See https://www.facebook.com/luleaDataCenter

215 See http://www.facebook.com/safety/groups/law/guidelines/

of a Facebook account.[216] In effect, the interests of the state where the cloud data is stored lose relevance in relation to the interest of the state on whose territory the data is 'controlled.'[217]

Such challenges were highlighted by countries during information gathering for the Study. When asked, for example, about obtaining electronic evidence from service providers located in another jurisdiction, a number of countries commented that the process of obtaining extra-territorial data is lengthy, with difficulties in locating '*foreign authorities with both the legal authority and technical expertise in the places where digital evidence is physically located.*'[218]

International and regional approaches

The challenges of obtaining extra-territorial data controlled by third parties have been recognized for a long time. During the drafting of the Council of Europe Cybercrime Convention, for example, Article 32 was included with the aim of allowing Parties, without the authorization of another Party, to: (a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; and (b) to access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.[219] An article has since been included in almost identical terms in the League of Arab States Convention.[220]

As it is particularly relevant to the obtaining of extra-territorial data in law enforcement investigations, this discussion focuses on the actions described by Article 32(b) of the Council of Europe Cybercrime Convention (access to stored data with consent). Such actions are commonly termed 'trans-border' access.

Article 32(b) is drafted in permissive terms, insofar as it envisages that States parties to the Council of Europe Cybercrime Convention *may* undertake such actions. It does not directly prohibit States parties from preventing other States parties so accessing data stored in their territory – but were a State party to do so, this could be considered incompatible with the spirit of the Article. Access '*without authorization*' of another State party is interpreted as '*to unilaterally access computer data stored in another Party without seeking mutual assistance.*'[221] The Article is silent on the point of notification to the other Party – neither prohibiting it nor requiring it. It should also be noted that Article 32(b) concerns the access or receipt of stored 'computer data' in general, and is not limited to the context of cybercrime investigations. One perspective is that Article 32(b) constitutes a rule validly permitting the exercise of state power on the territory of another within the exceptions foreseen by international law.[222] Another is that such access is incompatible with the principle of sovereignty and non-interference, if carried out without the consent of the state on whose territory the data is stored.[223] A third perspective is that such actions do not meet the threshold of 'interference' in the internal or external affairs of the state on whose territory the data is stored.[224]

---

216 *Ibid.*

217 Sieber, U., 2012. *Straftaten und Strafverfolgung im Internet. Gutachten C zum 69. Deutschen Juristentag.* Munich: C.H. Beck.

218 Study cybercrime questionnaire. Q105.

219 See, Council of Europe Cybercrime Convention, Art. 32.

220 See, League of Arab States Convention, Art. 40.

221 Council of Europe, Cybercrime Convention Committee (T-CY), Ad-hoc Sub-group on Jurisdiction and Transborder Access to Data, 2012. *Transborder access and jurisdiction: What are the options?* T-CY (2012)3. 6 December, p.21.

222 *Ibid.* At p.27, citing '*a permissive rule derived from international custom or convention*' as contained in the *Lotus* case, PCIJ Series A., No.10, at 18 (1927).

223 Sieber, U., 2012. *Straftaten und Strafverfolgung im Internet. Gutachten C zum 69. Deutschen Juristentag.* Munich: C.H. Beck.

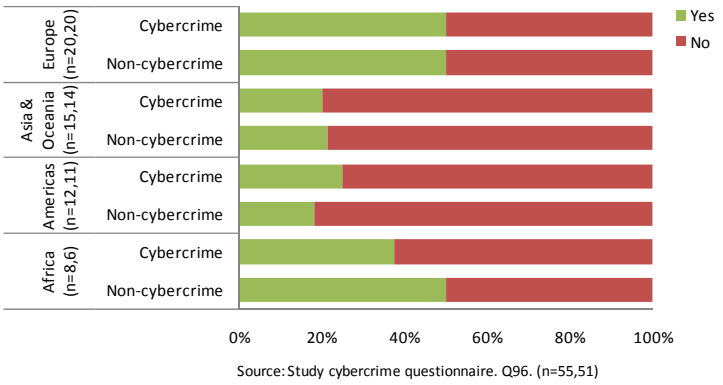
224 Council of Europe, Cybercrime Convention Committee (T-CY), Ad-hoc Sub-group on Jurisdiction and Transborder Access to Data, 2012. *Transborder access and jurisdiction: What are the options?* T-CY (2012)3. 6 December, p.27.

Cloud computing was certainly not as developed at the time of the drafting of Article 32 of the Council of Europe Cybercrime Convention. Nonetheless, the drafters specifically envisaged the application of Article 32(b) to, amongst others, the situation where '*a person's e-mail may be stored in another country by a service provider.*'[225] As such, Article 32(b) conceivably applies in wide range of circumstances, including accessing or receiving computer data from extra-territorial individuals; private sector organizations; service providers; and – in today's world – cloud service operators. A potential advantage of Article 32(b) to law enforcement is that, if lawful and voluntary consent is contained, investigators do not have to follow mutual legal assistance procedures that move too slowly for capture of transient data.

National practice

During information gathering for the Study, countries were asked about the use of 'trans-border access to a computer system or data' as an investigative measure,[226] and about whether 'trans-border access' to a computer system or data within the country by foreign law enforcement was permitted.[227]

Figure 7.17: Police use of trans-border access for investigation of cybercrime and other crimes



Source: Study cybercrime questionnaire. Q96. (n=55,51)

With respect to use of 'trans-border' access by law enforcement authorities, around 20 per cent of countries in the Americas, and Asia and Oceania reported that the measure was used, either for the investigation of cybercrime or other crimes. This rose to around 40 per cent of responding countries in Africa, and 50 per cent in Europe.[228] The higher percentage in Europe may reflect the influence of Article 32(b) of the Council of Europe Cybercrime Convention.

In responding to the questionnaire, however, countries placed a wide meaning on the term 'trans-border' access – with some countries including the situation where direct access to extra-territorial data was carried out, but only after approval had been received from the foreign authorities.[229] A number of countries referred to particular restrictions on the practice, such as a need to obtain the consent of the owner, notifiction conditions, and a requirement to ensure that the data is actually stored abroad. Countries that did not make use of the practice frequently cited a lack of legal framework as the main reason for not doing so. Some countries highlighted in particular that they were constrained in gathering evidence abroad to the use of mutual legal assistance and letters rogatory.[230]

Concerning passive interception sites in one country monitoring wireless communications from a foreign country, see also, ECtHR. Application No. 54934/00. 29 June 2006, in which the Court found that the respondent country had not acted in a manner which interfered with the territorial sovereignty of foreign states as protected in public international law.

225 Council of Europe, 2001. *Explanatory Report to Convention on Cybercrime.*

226 Study cybercrime questionnaire. Q96.

227 Study cybercrime questionnaire. Q108.

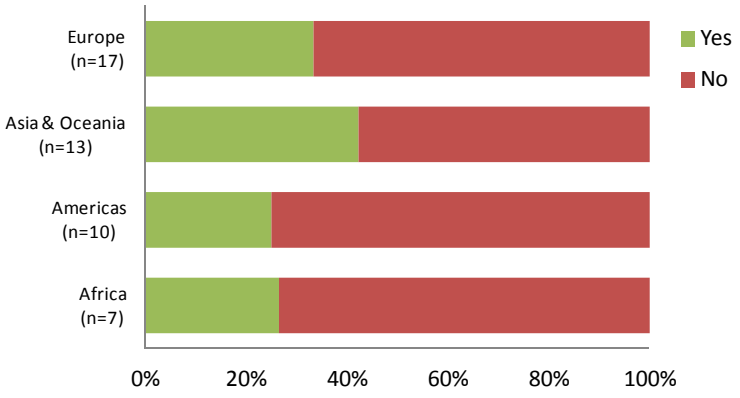
228 *Ibid.*

229 *Ibid.*

230 *Ibid.*

As regards the permissibility of foreign law enforcement access to computer systems or data, aound two-thirds of countries in all regions of the world stated that this was not permissible.[231] One country from Oceania, for example, stated that national law enforcement authorities could '*access computer systems and computer data on behalf of a foreign country through formal mutual legal assistance processes*,' although the scope of assistance '*is limited to situations where a search warrant is executed on [national] premises […]*,' and national authorities are unable '*to access stored communications on behalf of a foreign country.*'[232] Other countries perceived that the practice was incompatible with the principle of sovereignty of states. Where countries do allow trans-border access to computer systems or data within their territory, this was often stated to be only as provided for by the Council of Europe Cybercrime Convention. One country noted that the practice was permissible on the basis of reciprocity. In other cases, such as for one country in South America, the practice is permissible '*in urgent cases involving a serious crime that threatens the integrity or life of a person.*'[233] Other countries reported that trans-border access was permissible '*if the matter threatened national security*.' One country in Northern Europe stated that it will allow for access '*if it is impossible to know* [*in which country*] *the data actually is.*'[234]

Figure 7.18: Permissibility of trans-border access to computer system or data by foreign law enforcement



Source: Study cybercrime questionnaire. Q108. (n=47)

In practice, it appears that when obtaining extra-territorial data, the majority of responding countries rely on formal channels – necessitating requests for mutual legal assistance.[235] Overall, less than 10 per cent of countries reported 'most often' contacting extra-territorial service providers directly for evidence such as subscriber, traffic or content data.[236] One country in Western Asia observed that initiating contact with an extra-territorial service provider would be carried out in an informal manner, and, if the provider refused cooperation, law enforcement authorities would revert to formal channels in order to obtain the necessary permissions and the requested data.[237]

Conceptualizing direct access to extra-territorial data

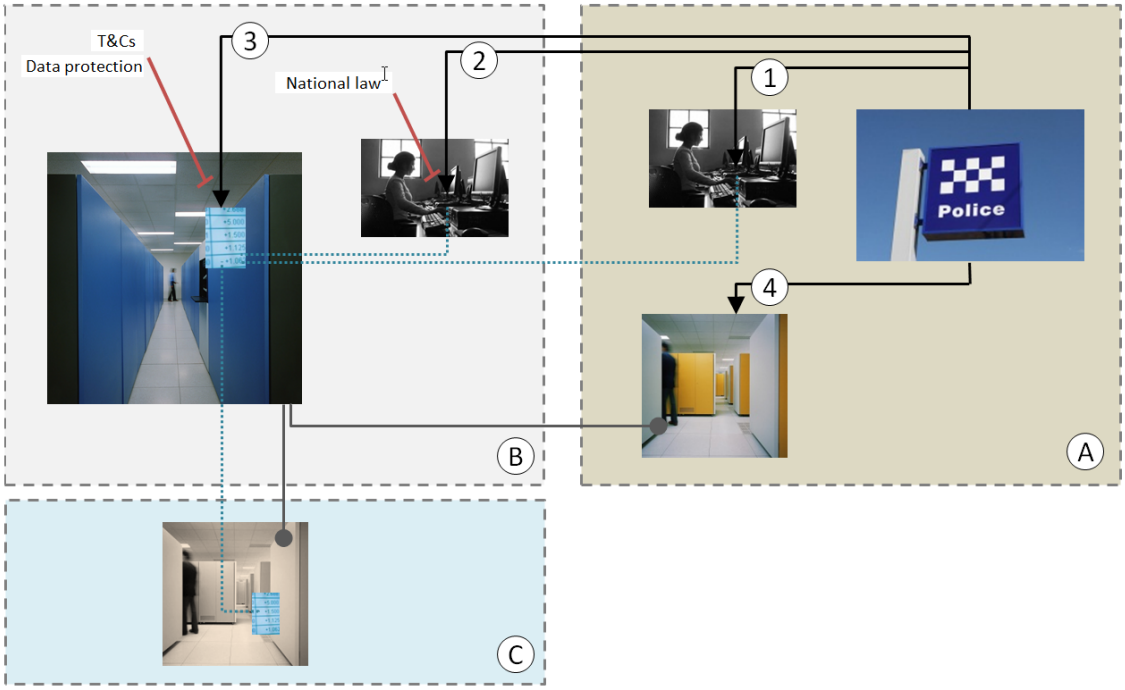
In order to conceptualize the considerations involved in access to extra-territorial data without a formal mutual legal assistance request, or other police-to-police informal cooperation, the figure below demonstrates four possible scenarios in the context of cloud computing.

The example involves a cloud service provider with head office and data centres in country B, but with additional data centres in country C, and further offices in country A. Law enforcement authorities in country A access or receive cloud data believed to be stored in country B, via:

231 Study cybercrime questionnaire. Q108.
232 *Ibid.*
233 *Ibid.*
234 *Ibid.*
235 Study cybercrime questionnaire. Q105.
236 *Ibid.*
237 *Ibid.*

(1) An individual located in country A with control over cloud data. Access may be obtained either because (i) the individual consents; or (ii) authorities make use of an existing live connection from the individual's device.
(2) An individual located in country B with control over cloud data. Access may be obtained due to the consent of the individual.
(3) The cloud service provider in country B. Access may be obtained either because (i) the cloud service provider consents; or (ii) data access credentials have been obtained by law enforcement.
(4) The cloud service provider's offices in country A. Access may be obtained through local informal arrangements between law enforcement and the cloud service provider.

In all situations, while the data is believed by law enforcement to be held by the cloud service provider in its data centres in country B, it is also possible that the data, or a copy of it, may be physically located in country C. In other possible examples, law enforcement authorities in country A may have no initial information at all about the location of data – including whether it is physically extra-territorial or not.[238]



The range of possibilities demonstrates the complexity of law enforcement direct access to extra-territorial data. Within the example, further nuances also exist, including: (i) the effect of the cloud service provider's customer terms and conditions on foreign law enforcement requests; (ii) the lawfulness in country B of interactions between foreign law enforcement, and individuals and legal persons within the territory; and (iii) the lawfulness in country A of the way in which any access credentials are obtained by law enforcement.

Consideration of a range of similar scenarios in a recent report by the Council of Europe found a number of differences in state approaches. These included with reference to: whether it was apparent to investigators that data was stored in a different jurisdiction; whether investigators were permitted to obtain remote access by means of software such as key loggers and sniffers; whether a

238 During 'live' access of a suspect's device for example, it may not be clear whether data is stored (or 'cached') locally on the device, accessed via a network connection to a server within the territory, or accessed via a network connection to a server outside of the territory.

person providing access has lawful authority to dicslose the data under the laws where the data is stored; and whether it makes a difference if the person providing access is physically located in the requesting state or extra-territorially.[239]

Key considerations

The conceptual example considered above, together with the answers of countries to the Study questionnaire, highlight a number of key considerations.

Firstly, it is apparent that law enforcement authorities may, in practice, directly access extra-territorial data *without the consent* of either an individual or the service provider. This could occur for example, where investigators make use of an existing live connection from a suspect's device, or where investigators use lawfully obtained data access credentials to access cloud data.

Secondly, law enforcement authorities carrying out such actions will not always know *whether* the data access is in fact extra-territorial or, if it is, in *which* country or countries the data is physically located. This can occur, for example, where cloud computing providers store data in multiple copies in data centres in different countries, and make use of dynamic data management between these data centres.

Both of these points have relevance to existing international and regional approaches such as the provisions of Article 32(b) of the Council of Europe Cybercrime Convention, and Article 40(2) of the League of Arab States Convention – both of which require the *consent* of a person who has lawful authority to disclose the data, and are limited to envisaging access to data *located in another Party*. Such provisions would not cover the situation where consent is not obtained and the data is physically located in a country which is not party to the relevant instrument.

In particular, with respect to the issue of *consent* and cloud computing providers – many responding countries indicated that service providers operating within their jurisdiction were only obliged to disclose data upon receipt of a court order, subpoena or warrant.[240] These obligations apply equally – if not even more so – to foreign law enforcement requests. A number of service providers that responded to the Study noted that they do not consider informal requests from foreign law enforcement authorities to generate any obligation to disclose data.[241] Overall, companies that responded to the Study noted that they preferred to receive formal requests through regimes based on mutual legal assistance treaties. Examination of guidelines from online service providers also demonstrates this approach. Law enforcement guidelines from Twitter, for example, state that *'…law authorizes Twitter to respond to requests for user information from foreign law enforcement agencies that are issued via …court either by way of a mutual legal assistance treaty or a letter rogatory.'*[242] As such, foreign law enforcement authorities may find it challenging to obtain data from an extra-territorial service provider by direct consent.

The picture adds up to one of a complex balance. On the one hand, some sovereignty and individual privacy arguments suggest that access to extra-territorial computer data is only appropriate through mutual legal assistance procedures – which entail formal consideration of such issues on a case-by-case basis.[243] On the other hand, law enforcement realities indicate that, through

---

239 Council of Europe, Cybercrime Convention Committee (T-CY), Ad-hoc Sub-group on Jurisdiction and Transborder Access to Data, 2012. *Transborder access and jurisdiction: What are the options?* T-CY (2012)3. 6 December 2012. p.29-31.

240 Study cybercrime questionnaire. Q21.

241 Study cybercrime questionnaire (private sector). Q28.

242 See http://support.twitter.com/articles/41949-guidelines-for-law-enforcement#

243 This recommendation was made, for example, by Global Network Initiative, 2012. *Digital Freedoms in International Law: Practical Steps to Protect Human Rights Online.*

a number of means, direct access to extra-territorial data does occur, *in practice*, in the course of investigations – either with or without the knowledge of investigators. Driving forces for this include the length of time required for formal cooperation procedures; situations where devices with live connections are encountered; and where access credentials become known in the course of an investigation.

Current international and regional approaches present a number of limitations through a focus on 'consent' and presumed knowledge of the 'location' of data. In reality, 'true' data location is rarely known at the outset of an investigation, or at the point at which data access may be required. Even where formal mutual legal assistance requests are used, these may be directed to the jurisdiction of the *seat* of the cloud service provider, rather than the jurisdiction of the *physical* data centre.[244]

From a crime prevention and criminal justice perspective, a number of circumstances exist in which urgent access to cloud data can be required – including where there is an imminent threat of harm. Achieving consensus on the most effective way in which this might be achieved while ensuring respect for individual human rights[245] will require: (i) (re)-conceptualization of the extent to which 'data location' can still be used as a guiding principle; and (ii) the development of common standards and safeguards concerning the circumstances, if any, under which direct access to extra-territorial data may be conducted by law enforcement.

244 Conceivably, agreements between operators of data centres owned by global companies and host countries could address this point.

245 See Chapter Five (Law enforcement and investigations), Section 5.3 Privacy and investigative measures.

Page left intentionally blank

CHAPTER EIGHT: PREVENTION

This Chapter takes a holistic look at cybercrime prevention from the perspective of governments, the private sector and academia. It finds many important links between these stakeholders and emphasizes a range of interactions between them that can lead to effective cybercrime prevention measures.

8.1 Cybercrime prevention and national strategies

KEY RESULTS:

- Almost 40 per cent of responding countries report the existence of national law or policy on cybercrime prevention. Initiatives are under preparation in a further 20 per cent of countries
- Good practice includes the promulgation of legislation, effective leadership, development of criminal justice and law enforcement capacity, education and awareness, the development of a strong knowledge base, and cooperation across government, communities, the private sector and internationally
- Around 70 per cent of all countries reported national strategies included components on awareness raising, international cooperation, and law enforcement capacity
- Over 50 per cent of responding countries reported having established public-private partnerships for the prevention and combating of cybercrime

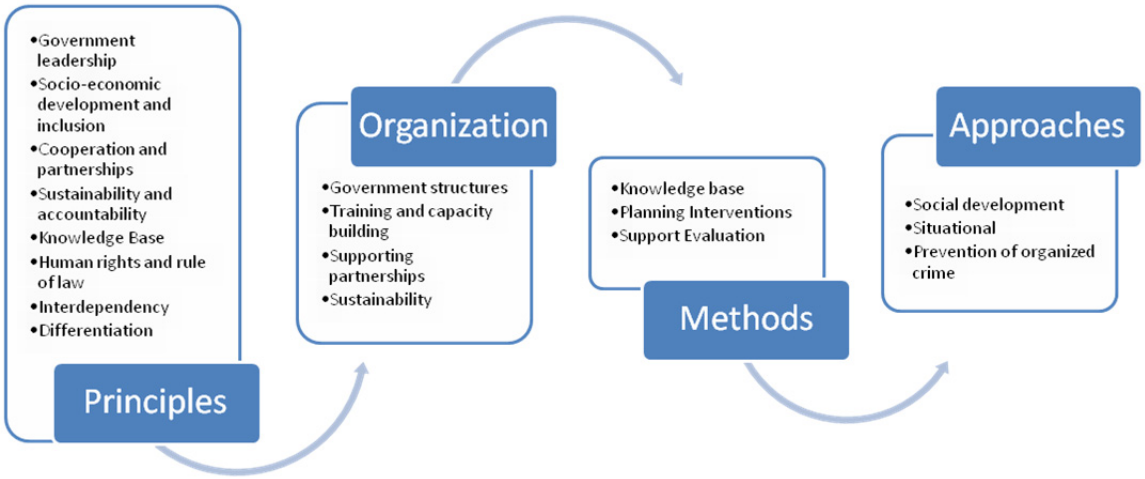
Introduction to crime prevention

'Crime prevention' refers to the strategies and measures that seek to reduce the *risk* of crimes occurring, and their potential harmful effects on individuals and society, through interventions that influence the multiple causes of crime.[1] The United Nations Guidelines for the Prevention of Crime highlight that government leadership plays an important part in crime prevention, combined with cooperation and partnerships across ministries and between authorities, community organizations, non-governmental organizations, the business sector and private citizens.[2] Good crime prevention practice starts with basic *principles* (such as leadership, cooperation, and the rule of law), suggests forms of *organization* (such as crime prevention plans), and leads to the implementation of *methods* (such as development of a sound knowledge base) and *approaches* (including reducing criminal opportunities and target hardening).

1 *Guidelines for the Prevention of Crime*, annex to United Nations Economic and Social Council Resolution 2002/13 on *Action to promote effective crime prevention,* 24 July 2002, para. 3.

2 *Ibid.* Arts. 7 and 9.

Figure 8.1: Crime prevention principles, organization, methods, and approaches

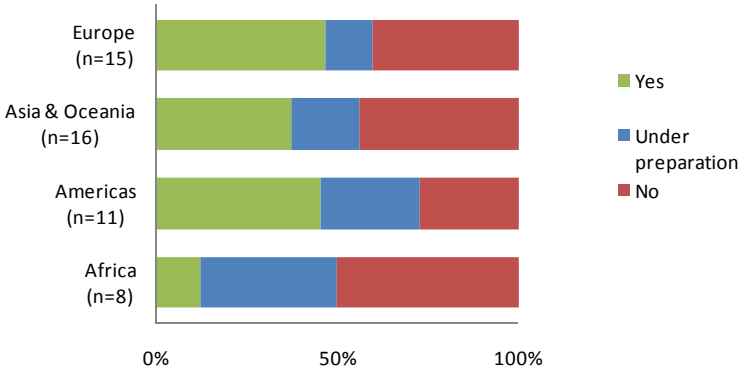


Cybercrime presents particular crime prevention challenges. These include the increasing ubiquity and affordability of online devices leading to large numbers of potential victims; the comparative willingness of persons to assume 'risky' online behaviour; the possibility for anonymity and obfuscation techniques on the part of perpetrators; the transnational nature of many cybercrime acts; and the fast pace of criminal innovation. Each of these challenges has implications for the *organization, methods* and *approaches* adopted for cybercrime prevention. Organizational structures, for example, will need to reflect the need for international and regional cooperation in cybercrime prevention. *Methods* will need to ensure a constantly updated picture of cyber threats, and *approaches* will need to involve a range of stakeholders – in particular the private sector organizations that own and operate internet infrastructure and services.

National approaches to cybercrime prevention

An integral part of the *organizational* aspect of crime prevention is the establishment of a crime prevention *plan* with clear priorities and targets.[3] The Guidelines for the Prevention of Crime state that governments should include prevention as a permanent part of their structures and programmes for controlling crime, and ensure that clear responsibilities and *goals* exist within government for the organization of crime prevention.[4]

Figure 8.2: National legislation or policy for cybercrime prevention



Source: Study cybercrime questionnaire. Q8. (n=50)

During information gathering for the Study, around 40 per cent of responding countries indicated the existence of national legislation or policy on

[3] *Guidelines for the Prevention of Crime*, annex to United Nations Economic and Social Council Resolution 2002/13 on *Action to promote effective crime prevention*, 24 July 2002, para. 17.

[4] *Ibid.*

cybercrime prevention.[5] A further 20 per cent of countries indicated that law or policy was under development. Countries in Europe and the Americas most often reported the existence of a law or policy on prevention. Few countries in Africa reported the existence of a prevention law or policy, although around 40 per cent of responding countries from Africa reported that such an instrument was under development. Globally, however, the fact that more than half of all responding countries confirmed that no national legislation or policy for cybercrime prevention is in existence indicates significant potential for strengthening responses in this area.

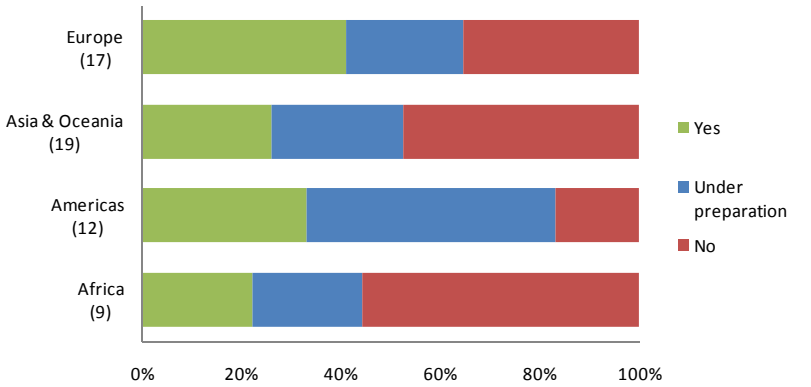
For those countries with laws or policy on cybercrime prevention, countries reported that cybercrime prevention laws and policies were typically designed '*to organize and co-ordinate the legal environment, to establish effective and coordinated institutional systems, to assign responsibility for different aspects of cybercrime, and to prepare awareness programs for users, technical personnel and decision-makers'*.[6] Other countries also highlighted that prevention laws set out the different roles and responsibility of public institutions, service providers, and non-governmental organizations in cybercrime prevention programmes.

A number of countries – in both the developed and developing world – reported on specific cybercrime prevention or awareness activities undertaken, including through law enforcement agencies and other government institutions, academia, and private sector organizations. One country in South America, for example, reported work with internet service providers and internet cafés on regulatory compliance, as well as risk reduction activities in specific communities through the creation of crime prevention committees aimed at promoting the prevention of digital crime.[7] Other countries highlighted work with bank federations on enhancing internet security, the development of cybersecurity training in partnership with non-governmental organizations in schools, and the engagement of law enforcement agencies at conferences and other forums concerning cybercrime.[8] Countries further noted the importance of designating an easily accessible focal point for citizen and corporate reporting of cybercrime and for prevention advice. Cybercrime awareness raising activities are discussed in detail later in this Chapter.

Cybercrime strategies

Many countries framed responses related to cybercrime *prevention* within the overall context of the need for a national cybercrime *strategy.*[9] In turn, many countries also highlighted the strong links between *cybercrime* and *cybersecurity* strategies. When asked about the existence of a national strategy (or equivalent) 'for cybercrime', countries refered to all of

Figure 8.3: Existence of national cybercrime strategy



Source: Study cybercrime questionnaire. Q1. (n=57)

5 Study cybercrime questionnaire. Q8.
6 Study cybercrime questionnaire. Q8.
7 Study cybercrime questionnaire. Q9.
8 *Ibid.*
9 Study cybercrime questionnaire. Q1 and Q8.

'cyber' strategies, 'cybersecurity' strategies, 'information security' strategies, 'cyberspace' strategies, and 'cybercrime' strategies.[10] This range of responses highlights the increasing interdependence of citizen security and vulnerability to cybercrime, and the security of national computer infrastructure, as well as that of transnational corporations. While significant overlap exists between cybercrime and cybersecurity approaches, the two fields nonetheless also have some differences. These are summarized in the box on this page.

In so far as responding countries reported on a range of strategies relevant to cybercrime, the analysis in this Chapter is not limited to the 'strict' definition of a cybercrime strategy. Rather it seeks to reflect information provided through the Study questionnaire, encompassing all strategy types reported.

Cybercrime and cybersecurity strategies

National interests and security, trust, resilience, reliability of ICT		Rule of law, human rights, and crime prevention and criminal justice	
Cybersecurity strategies		**Cybercrime strategies**	
Non-intentional ICT security incidents	Intentional attacks against the confidentiality, integrity and availability of computer systems and data	Computer-related and content-related offences	Any offence involving electronic evidence

Adapted from Seger, A., 2011. *Cybercrime strategies. Octopus conference 2011.*

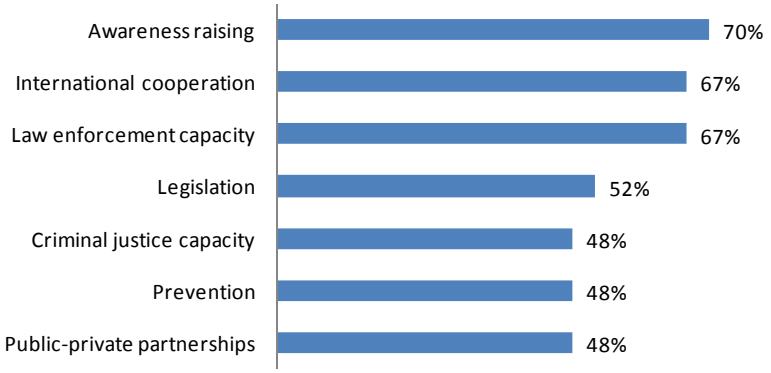
Overall, around 30 per cent of responding countries indicated the existence of a national cybercrime strategy (in the broadest sense). Depending upon the region, a further 20 to 50 per cent of countries reported that such a strategy was under preparation. Countries in Africa, Asia and Oceania reported the lowest levels of cybercrime strategies – with 50 per cent or more of countries indicating that such an instrument did not exist. Cybercrime strategies are important for ensuring that national law enforcement and criminal justice responses fully take into account both the particular challenges of cybercrime, as well as electronic evidence components of all crimes. The development of a cybercrime strategy represents a critical first step in determining operational and strategic priorities before engagement in processes such as legislative reform. As evidenced by the range of country responses, cybercrime strategies may be prepared as 'stand-alone' documents, or integrated as components of cybersecurity strategies.

During information gathering for the Study, countries were also asked about areas covered by national cybercrime strategies. Reported areas cover nearly all of those addressed in this Study – including cybercrime prevention and awareness raising, law enforcement and criminal justice capacity, public-private partnerships, legislation, and international cooperation. For the almost 30 national strategies regarding which information was provided, crime *prevention* represents a key component. Cybercrime 'prevention', in general terms, was included in almost half of all reported national strategies. In addition, the most commonly cited area covered by these strategies was the specific prevention activity of 'awareness raising' – with 70 per cent of reported strategies including this topic.[11] The next section in this Chapter examines this area in detail.

[10] Study cybercrime questionnaire. Q1.
[11] Study cybercrime questionnaire. Q1.

The next most commonly cited area within reported national cybercrime strategies was 'international cooperation'. The strategic importance of this area, including from the crime prevention perspective, was highlighted by a number of countries. One noted that: '*International cooperation is seen as the very core of*' '*the exceptional challenges posed by transnational, high-speed, sophisticated and pervasive cybercriminality for all Member States who must balance the need for rapid and effective investigative and law enforcement measures against the protection of national sovereignty, the respect for comity and the need to ensure the protection of the human rights of persons within their jurisdictions.*'[12] International cooperation in criminal matters involving cybercrime is discussed in detail in Chapter Seven (International cooperation) of this Study.

Figure 8.4: National cybercrime strategy areas



Source: Study cybercrime questionnaire. Q1. (n=27, r=108)

The same proportion (almost 70 per cent) of countries also included 'law enforcement capacity' as a key area of their national cybercrime strategy. Reported challenges to law enforcement capacity were succinctly described by one country as '*equipment, capacity, and human resources.*'[13] Chapter Five (Law enforcement and investigations) of this Study examines this area in greater detail. Other areas featured in national cybercrime strategies included cybercrime legislation, and criminal justice capacity. A concerted focus emerged on establishing capacity and education for prosecutors, magistrates, and judges. A few countries identified specific goals and plans, such as to place '*at least one public prosecutor solely responsible for cyber crime cases in all court districts by 2015*'[14] or to '*create a pool of judicial experts from public and private sectors to share expertise and knowledge*'.[15] Chapter Six (Electronic evidence and criminal justice) examines this area.

A further theme commonly identified in cybercrime prevention priorities was the importance of protecting critical national infrastructures. This was noted to include the '*development of information and cybersecurity standards and awareness, as well as mechanisms to identify and mitigate cyber threats.*'[16] In this respect, cooperation between federal and local government and other sectors, in particular, was described as essential to '*facilitate information sharing relating to best practices, investigative information, coordination of incident response, and incident management, procedures, and processes*'[17].

Cybercrime leadership

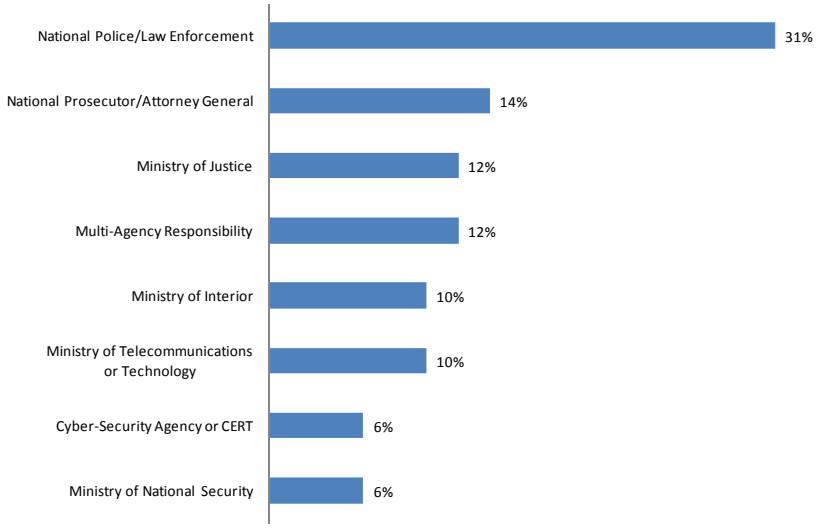
Responding countries recognized that a range of government institutions and agencies are required to support crime prevention and criminal justice responses in the area of cybercrime. However, many countries also noted that cybercrime prevention requires centralized leadership and enhanced resources for coordinating government cybercrime prevention initiatives.[18] Some 75 per

12 Study cybercrime questionnaire. Q4.
13 Study cybercrime questionnaire. Q5.
14 *Ibid.*
15 *Ibid.*
16 *Ibid.*
17 *Ibid.*
18 *Ibid.*

cent of responding countries reported that they had appointed a lead government institution responsible for coordinating the prevention and combating of cybercrime.[19] The most commonly reported institution (around 30 per cent of responding countries) was national police or law enforcement authorities. Other commonly identified lead institutions included offices of the prosecutor or attorney general, and ministries of justice. In just over 10 per cent of countries, a 'multi-agency' coordination lead was reported.[20]

In a small proportion of countries (around or under 10 per cent) the lead cybercrime coordination role was reported to lie with ministries of telecommunications, cybersecurity agencies, or CERTs, rather than with crime prevention and criminal justice institutions.[21] CERTs play a key role in identifying and mitigating computer system vulnerabilities, and in responding to computer security incidents.[22] As a result, they can possess important insights into current cybercrime trends. The use of ministries of telecommunications and CERTs as cybercrime lead highlights the multi-disciplinary nature of the cybercrime response.

Figure 8.5: Lead institution for coordinating cybercrime response



Source: Study cybercrime questionnaire. Q2. (n=51)

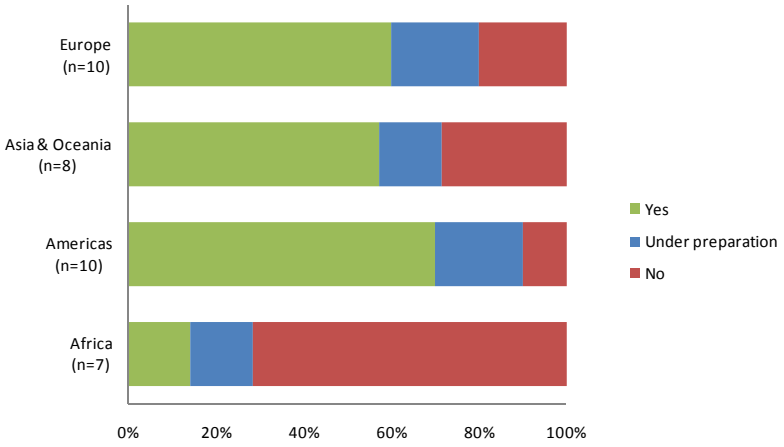
However, it is notable that, for the most part, coordination lead reflects the characterization of cybercrime primarily as a law enforcement and criminal justice challenge, rather than a 'communications and technological' challenge. Nonetheless, cybercrime has elements of both, and recent work at the European level suggests that cooperation between the CERT community and law enforcement is important in the areas of incident response and information sharing.[23] This aspect was also emphasized by countries responding to the Study questionnaire. Countries frequently reiterated, for example, the importance of a collaborative approach due to the complexity of cybercrime threats, including to critical and economic infrastructure. In this respect, identified challenges to effective coordination of cybercrime prevention activities included a lack of official statistics and reliable data about the extent of cybercrime, a lack of relevant legislation, and a '*lack of information sharing, coordination and cooperation among stakeholders and overlapping roles of IT Government Bodies.*'[24]

19 Study cybercrime questionnaire. Q2.
20 *Ibid.*
21 *Ibid.*
22 World Telecommunication Standardization Assembly, 2012. *Resolution 58* - Encourage the creation of national computer incident response teams, particularly for developing countries.
23 ENISA, 2012. *The Fight against Cybercrime: Cooperation between CERTs and Law Enforcement Agencies in the fight against Cybercrime. A first collection of practices.*
24 Study cybercrime questionnaire. Q5.

Public-private partnerships

In addition to partnership and coordination *within* government, responding countries across all regions highlighted the importance of *public-private* partnerships. Overall, over 50 per cent of responding countries reported having established public-private partnerships for the prevention and combating of cybercrime. Just under 20 per cent of responding countries reported that partnerships were under preparation. Around 30 per cent of responding countries stated that no public-private partnerships were in existence.[25]

Figure 8.6: Existence of public-private partnerships



Source: Study cybercrime questionnaire. Q6. (n=41)

The majority of countries reporting that partnerships did not exist were located in Africa, Asia, and Oceania. In particular, over 60 per cent of responding countries from Africa reported an absence of public-private partnerships. This picture is reversed for countries in Europe and the Americas, where 60 per cent or more of responding countries reported the existence of relevant partnerships.

Countries indicated a number of motivating factors for the establishment of partnerships, including the need to understand an evolving threat landscape, and a need to engage closely with private sector owners and operators of digital infrastructure.[26]

During information gathering for the Study, private sector organizations were also asked about the existence of public-private partnerships for the prevention and combating of cybercrime. Just over half of responding corporations indicated that they participated in such initiatives.[27] Such partnerships were typically reported with international

Models for cybercrime public-private partnerships

Legal frameworks, trust, incentives, and other factors are critical as enablers for a robust public-private cybersecurity partnership model to flourish. An appropriate focus is to analyse the best model for a successful partnership in context that can minimize challenges and provide the greatest benefit. Five primary models have emerged:

- Non-profit information sharing at global level
- Distributed information sharing at community level
- Centralized information sharing at community level
- Closed government
- Industry informal collaboration

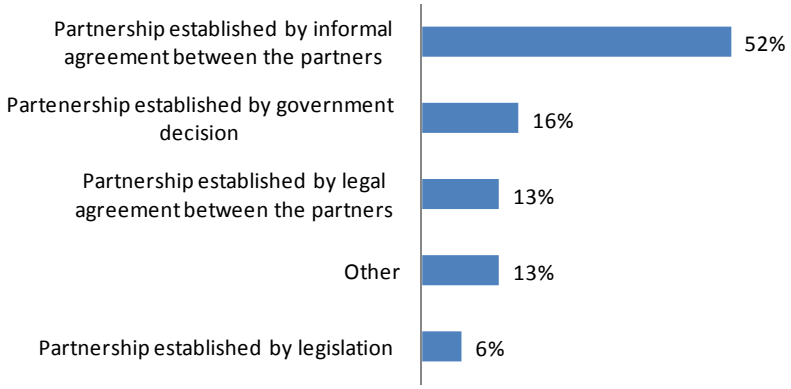
Key features of a successful partnership may include platform neutrality, authority, rules for data sharing, trust, non-open membership, encouragement of benefits and responsiveness.

Source: 17 ECLR 1936, 31 Dec 2012.

25 Study cybercrime questionnaire. Q6.
26 Study cybercrime questionnaire. Q6.
27 Study cybercrime questionnaire (private sector). Q40-45.

organizations, academic institutions, ministries of justice, law enforcement authorities, ministries of national security, and ministries of telecommunications.[28] Corporations reported many positive experiences of partnerships, including possibilities to exchange information on cybercrime threats and trends and on good practice in cybercrime prevention.[29] A number also referred to challenges in the establishment and maintenance of partnerships. Some corporations, for example, highlighted possibilities for '*divergent goals*' between private sector and government authorities, and explained that public-private partnerships needed to ensure that '*information sharing was a two-way street.*'[30] In this respect, a number of multinational private sector organizations emphasized that partnerships must focus on '*mutual solutions*', including in the areas of regulation, and crime prevention.[31]

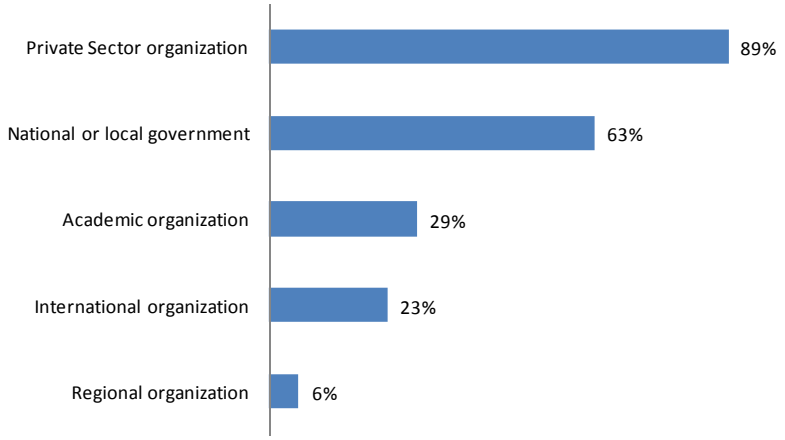
Figure 8.7: Public-Private Partnership Basis



Source: Study cybercrime questionnaire. Q6. (n=31)

Over half of responding countries indicated that public-private partnerships are created by informal agreement between the partners, indicating the non-binding nature of many such arrangements. Those partnerships established by formal government decision tended to more often involve corporations that deliver critical infrastructure, such as utilities and telecommunications.[32] Remaining reported partnerships were based on legal agreements between the partners, or other mechanisms, including memoranda of understanding and 'task force' membership. Legislation was the least commonly reported basis (just over five per cent) for organizing and advancing partnership activities. This corresponds with the use of public-private partnerships as dynamic responses based on issues of mutual interest, operational needs, and a need to respond to evolving cybercrime trends.

Figure 8.8: Partners in partnerhips



Source: Study cybercrime questionnaire. Q6 (n=35, r=73)

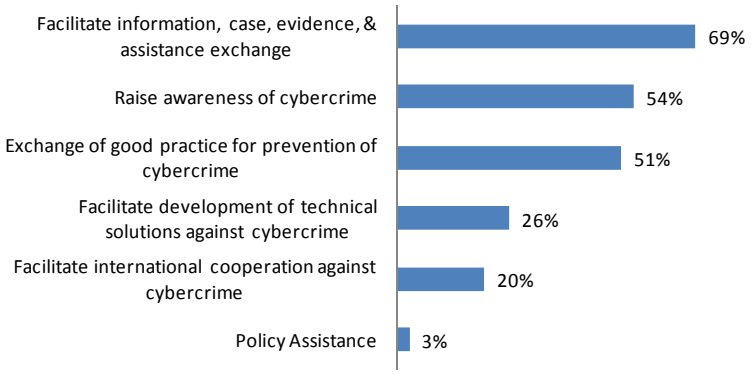
In line with information received from private sector organizations, responding countries reported that corporations were the most common participants in partnerships. Some 90 per cent of

28 *Ibid.*
29 *Ibid.*
30 Study cybercrime interviews (private sector).
31 *Ibid.*
32 Study cybercrime questionnaire. Q6.

all reported partnerships involved the private sector. In addition, academic, international and regional organizations were mentioned by a number of countries.

Partnership scopes reflected a range of activities. Almost 70 per cent of partnerships reported by countries were described as including the exchange of information on cybercrime. Countries reported, for example, that partnerships were used for '*facilitating evidence gathering*' and '*collaborative determination of working protocols and standards*', including '*establishing single points of contact.*'[33] When asked about the nature of information exchange in such partnerships, most countries reported that this concerned information on cybercrime threats and trends or general information on types of cybercrime cases. Half of responding countries also indicated, however, that information exchanged included information on *specific* cases of cybercrime acts. As noted in Chapter Five (Law enforcement and investigations), durable and efficient relationships between law enforcement and service providers can greatly assist effective cybercrime investigations. However, if such arrangements involve informal exchange of personal data, it is critical that they also meet rule of law and international human rights standards concerning legal certainty and guarantees against abuse.[34]

Figure 8.9: Scope of public-private partnerships



Source: Study cybercrime questionnaire. Q6 (n=35, r=78)

Other common partnership activities reported included the purposes of raising awareness of cybercrime, exchange of good practice for cybercrime prevention, and facilitating the development of technical solutions against cybercrime.[35] '*Sharing good practice methods*', for example, was cited as a partnership activity by half of respondents. Only a small percentage of reporting member states indicated that partnerships facilitated assistance in policy development. In light of private sector interest in mutual development of cybercrime responses, this represents one area in which public-private partnerships may further develop.

33 Study cybercrime questionnaire. Q6.
34 See Chapter Five, Section 5.3 Privacy and investigative measures.
35 Study cybercrime questionnaire. Q6.

8.2 Cybercrime awareness

KEY RESULTS:

- Surveys, including in developing countries, demonstrate that most individual internet users now take basic security precautions
- All stakeholders highlight the continued importance of public awareness-raising campaigns, including those covering emerging threats, and those targeted at specific audiences, such as children
- User education is most effective when combined with systems that help users achieve their goals in a secure manner

Raising awareness

The United Nations Guidelines for the Prevention of Crime highlight the importance of public education and awareness.[36] Increased public awareness of victimization risks and protective measures that can be taken represents an important strategy in the prevention of any crime type.[37] In addition to governments, during information gathering for the Study, private sector organizations also highlighted the importance of public and corporate awareness regarding cybercrime. One large telecommunications company for example, noted that: '*We must educate people about basic security. The owners of machines without basic security, patches, or updates are leaving their doors wide open. That campaign should be part of the government's role as well; we've got to continually message about people serving as their own best protection.*'[38]

Many countries reported awareness raising initiatives. One responding country in the Americas, for example, noted the importance of '*advertising campaigns in media, implementation of 24/7 interactive online chat portals,* [*and*] *strengthening social networks and websites*'.[39] A number of countries in the Americas and Europe also reported that they had developed strategies to raise awareness through dedicated campaign periods such as '*cyber security awareness month*' and '*internet safety day.*'

One country further reported that they had '*created a page on Facebook, which publishes… cyber security tips online and has links to a portal for reporting complaints. There is also the telephone number 1800-CRIME for reporting cybercrime incidents.*' A country in Europe noted that '*Measures to improve reporting of cybercrime have been further developed in 2007 with the creation of a specialized website… The site serves as a two-way information platform, where a person can get informed about the dangers encountered in the internet space, and on the other hand submit reports on committed crime. The reports are directly assigned to* [*police*] *officials… At present, around 150 reports monthly are received through the site… After the start of the campaign for promoting the site, it is expected that the visits to the site and the number of submitted reports will increase.*'[40] The table below summarizes details of four awareness campaigns reported during information gathering for the Study.

---

36 United Nations Guidelines for the Prevention of Crime. 2002. Economic and Security Council resolution 2002/13, Annex. Para.6 and 25.
37 See, for example, UNODC. 2010. Handbook on the crime prevention guidelines: Making them work.
38 Study cybercrime interview (private sector). June 2012.
39 *Ibid.*
40 *Ibid.*

Features of awareness-raising campaigns

	Campaign #1	*Campaign #2*	*Campaign #3*	*Campaign #4*
Funded and coordinated by	Government of a country in Northern Europe	Government of a country in Oceania	Government of a country in North America	Government of a country in South America
Key/Focal Features				
Safe use, ID theft, scams	✓	✓	✓	✓
Child protection, cyberbullying	✓	✓	✓	
Harmful content (violence, pornography, racism)	Within child protection	✓		
Private Sector – targeted campaigns, incl. financial sector (phishing, safety, etc.)				
Internet outreach				
Public Service Announcements, films	✓	Public service campaign		✓
Targeted Webpages	✓	✓	✓	
Interactive games		✓	Safe Online Surfing	
Alerts	RSS, Facebook, Twitter	Customized e-mail service		
Victim Information	✓			
Dedicated reporting portals	Action Fraud portal	Web portal		Web portal
Talks, briefings, outreach				
To citizens, general public	Annual week-long event, media campaigns	Annual awareness week	National Cybersecurity Awareness Month	Two-day conference
Special groups – students, teachers, professionals, academics, law enforcement, judiciary	Conferences, forums, meetings		National Cybersecurity Awareness Month	School outreach. Six-week basic training on the safe use of IT for IT specialists and students

Globally, a 2011 international review of cyber-security awareness raising and educational initiatives examined 68 such campaigns, all of which used the internet as a means of communication. Over one-third of the campaigns produced publications, and some 30 per cent included awareness raising days, weeks, or months, as well as training seminars and guidebooks. One quarter used videos and games or quizzes. Most campaigns were hosted by government agencies, although often as part of a consortium containing private sector and non-profit partners.[41]

[41] See http://www.acma.gov.au/webwr/_assets/main/lib310665/galexia_report-overview_intnl_cybersecurity_awareness.pdf

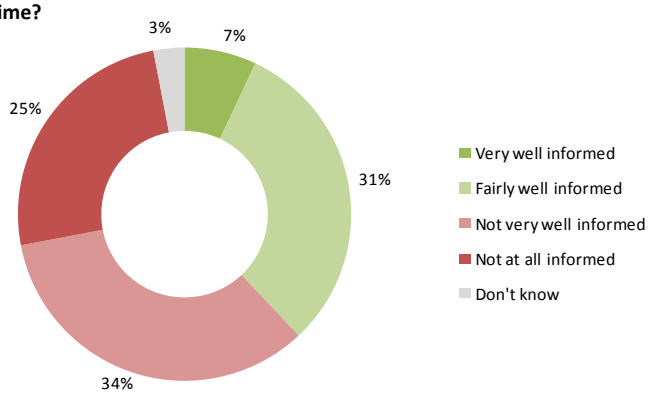
While many awareness campaigns are organized at national level, a small number of regional examples also exist. The European Information Sharing and Alert System, for example, was created in 2006. This campaign gathered information and educational materials from computer emergency response teams and other security communities from countries in Europe. Materials were then adapted for different groups of citizens and small and medium size businesses in each participating country. Materials were disseminated using social media, websites and mailing lists. A large-scale pilot focused on awareness of botnets, identity theft and social engineering threats reached over 1,500 people.[42]

Technology companies and non-profit groups have also run their own awareness-raising campaigns. Google's 'Good to Know' campaign, for example has run in around 40 languages since 2011. Adverts in newspapers, magazines, online and on public transport give security tips and explain some basic internet features such as cookies and IP addresses.[43] The Family Online Safety Institute has also worked with technology companies to aggregate educational resources for parents, children and teachers at their Platform for Good website.[44] Kyivstar, a telecommunications operator in Eastern Europe, ran a 'Tell Your Children about Internet Safety' campaign in April 2012, with adverts in print media, on vehicles and online, with volunteers also running information sessions in schools.[45] For a younger audience, Disney ran a TV, website and magazine safety campaign in 2012 aimed at 100 million children and parents in Europe, the Middle East and Africa.[46]

Despite a growing number of such campaigns, a number of countries reported the view that '*It will take a while for the public awareness campaigns to build up the public trust to increase cybercrime reporting*'.[47] The 2011 international review of campaigns further identified that few campaigns included an evaluation component. It also highlighted challenges in developing appropriate and cost-effective campaigns, and noted that providing information to users without additional training and skills acquisition activities can have a limited impact on their online behaviour. The review concluded that simple campaigns focused on a specific target group seemed to be most cost-effective.[48]

There is, accordingly, a need to understand underlying user risk behaviour, and perceptions of risk. Such information is important in the design and implementation of cybercrime awareness activities, as well as the prevention of cybercrime in general. The following section of this Chapter examines information from population-based and corporate surveys in this area.

Figure 8.10: How well informed do you feel about the risk of cybercrime?



Source: European Commission, 2012, Special Eurobarometer 390, July (p. 37)

Understanding user risk behaviour

Population-based surveys show that many internet users, at least in more developed countries, are 'aware' of cybercrime as

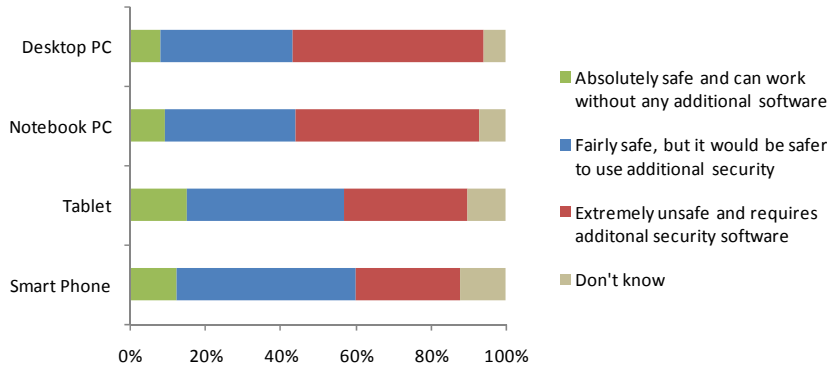
42 Degenhardt, W. 2012. *EISAS Large-Scale Pilot: Collaborative Awareness Raising for EU Citizens & SMEs*, ENISA.
43 See http://www.google.com/goodtoknow/
44 See http://aplatformforgood.org/
45 See http://en.csrukraine.org.ua/?p=367
46 See http://www.guardian.co.uk/technology/appsblog/2012/jul/04/disney-club-penguin-child-safety
47 Study cybercrime questionnaire. Q82.
48 Galexia. 2011. *An Overview of International Cyber-Security Awareness Raising and Educational Initiatives*. Australian Communications and Media Authority.

a risk. One survey in European countries, for example, showed that over 70 per cent of individuals had heard or seen information about cybercrime in the past year, mostly from television, newspapers, the Internet, the radio or from friends, family or colleagues.[49] Receipt of information about cybercrime did not, however, necessarily translate into 'feeling informed' about cybercrime. Only 7 per cent of respondents in the same survey reported feeling 'very well' informed about cybercrime. Over one half reported feeling 'not at all informed' or 'not very well informed'.

Nonetheless, surveys suggest that most computer users, including in developing countries, now take at least some basic security precautions. In one survey of over 13,000 internet users in 24 countries, almost 90 per cent of respondents reported deleting suspicious e-mails from unknown senders. Around 80 per cent of respondents reported using at least basic antivirus software, and not opening attachments or links in unsolicited e-mail or texts.[50] Only half of respondents, however, reported using social networks' privacy settings to control information sharing, with over 35 per cent having accepted 'friend requests' from people they do not know. Largely mirroring this pattern, another international survey of almost 4,000 internet users across six countries in North America and Europe found that around 10 per cent of e-mail users had clicked on potentially risky links in messages suspected to be spam, while just under 10 per cent had opened an attachment in a suspected spam message.[51]

Surveys of the younger generation in less developed countries show particularly high levels of cybercrime victimization risk. One survey of over 25,000 school-age children in seven countries in Central and South America reported that, of the approximately 45 per cent of children who had a home internet connection, only around 10 per cent of adolescents (10 to 18 years) reported having security software installed (either web filtering or anti-virus). Some 20 per cent of respondents did not know if they had security software installed or not.[52]

Figure 8.11: Perceived safety of device



Source: Kaspersky Lab, 2012. Perception and knowledge of IT threats (p. 2)

Security concerns and risk behaviour do not only apply to desktop computer use. As noted in Chapter 1 (Global connectivity), more users access the internet using a mobile device than fixed line broadband. Although electronic threats are becoming increasingly prevalent for mobile devices,[53] users still perceive that mobile devices and tablets are safer than desktop computers. One survey of 11,000 internet users in Latin and North America, Europe, the Middle East, Asia and Africa, for example, found that 60 per cent of users thought that it was 'safe' or 'fairly safe' to use a

49 European Commission. 2012 *Special Eurobarometer 390*.
50 Symantec. 2012. *Norton Cybercrime Report 2012*.
51 Messaging Anti-Abuse Working Group (MAAWG), *2010 Email Security Awareness and Usage Report*. New York: Ipsos Public Affairs. This survey was weighted to be representative of online population in each country.
52 Fundación Telefónica. 2008. *La generación interactiva en Iboamérica: Niños y adolescentes ante las pantallas*.
53 See, for example, Symantec. 2012. *Internet Security Threat Report*, Volume 17.

smart phone without additional security, compared to around 45 per cent for desktop and notebook computers.[54]

Limits of user education

Advice to individuals on cybercrime risks and mitigation is an important component of an overall cybercrime reduction strategy. However, there are limits as to how far users can be expected to learn complex security mechanisms, remember long and varied passwords for every online service they sign up to, and take other precautions that often directly interfere with the task at hand.[55]

Unsurprisingly, many users cannot or will not follow security advice that is a much greater burden than the likely individual consequences of a security failure. Security researchers note for example, that '*if users spent even a minute a day reading URLs to avoid phishing, the cost (in terms of user time) would be two orders of magnitude greater than all phishing losses.*'[56] Understanding all of the different ways in which a phishing site can impersonate a given domain would require a time and education investment that most users would be rational to reject.[57]

User education will likely be much more effective if combined with systems that help users achieve their goals in a secure manner. It should require deliberate confirmation when users attempt to take actions that can seriously compromise the security of their system – for example, by installing software of unknown origin. The user cost of security measures should be proportionate, however, to the benefit they bring – for example, complex password rules require user investment in remembering difficult passwords, but could easily be circumvented by key-logging or phishing attacks. If user cost is higher than direct user benefit, individuals have a strong incentive to ignore security measures.[58]

Within organizations and private sector corporations, organizational processes that promote security-conscious behaviour by employees and customers are thus critical – for example, by helping users to choose secure but memorable single sign-on passwords at a convenient time, and reinforcing that passwords will never be requested in a telephone call or e-mail, or after clicking on a link in e-mail messages. Social and organisational culture should avoid fostering the view that security-'wise' behaviour is 'paranoid' or 'pedantic' and interferes with productivity. Rather, organizational culture should help promote and reward secure behaviour.[59] The next section of this Chapter examines cybersecurity practices adopted by private sector organizations.

---

54 Kaspersky Lab. 2012. *Perception and knowledge of IT threats: the consumer's point of view*, p.2.

55 Sasse, M.A., Brostoff, S. and Weirich, D., 2001. Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security. *BT Technology Journal* , 19(3):122-131.

56 Herley, C., 2009. So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. New Security Paradigms Workshop, Oxford.

57 *Ibid.*

58 *Ibid.*

59 Sasse, M.A., S Brostoff and D Weirich (2001) Transforming the 'weakest link' — a human/computer interaction approach to usable and effective security. *BT Technology Journal* , 19(3):122-131.

8.3 Cybercrime prevention, the private sector and academia

KEY RESULTS:

- Private sector respondents report a range of cybersecurity awareness and actions. Two-thirds of private sector respondents had conducted a cybercrime risk assessment, and most reported use of cybersecurity technology
- Concern was expressed, however, that small and medium-sized companies either do not take sufficient steps to protect systems, or incorrectly perceive they will not be a target
- Some companies, including service providers and technology companies have taken proactive steps to counter cybercrime acts, including through the use of legal action
- Internet service providers and hosting providers can play a key role in cybercrime prevention. They may retain logs that can be used to investigate criminal activity; help customers to identify compromised computers; block some kinds of illegal content such as spam; and in general support a secure communications environment for their customers
- Academic institutions represent an important partner in cybercrime prevention through knowledge development and sharing; legislation and policy development; the development of technology and technical standards; the delivery of technical assistance; and cooperation with law enforcement authorities

This section examines three aspects of the relationship between the private sector, academia and cybercrime: (i) cybersecurity approaches adopted by private sector organizations; (ii) actions that internet service providers can take in the prevention of cybercrime; and (iii) the role of academia and intergovernmental organizations in cybercrime prevention.

Cybersecurity practices of private sector organizations

During information gathering for the Study, private sector organizations were asked about cybersecurity practices adopted with a view to preventing cybercrime victimization. Information received from corporations is presented here with reference to the OECD Guidelines for the Security of Information Systems and Networks.[60] The OECD guidelines have been reflected in a General Assembly Resolution concerning the creation of a Global Culture of Cybersecurity,[61] as well as in regional instruments[62]. They were also used by the International Chamber of Commerce to produce a short guide on '*information security assurance for executives*,' which notes that '*All parties have a role to play in a culture of security, but business, as the principal innovator, developer, user and provider of Information and Communication Technologies (ICT), has a broader role than most.*'[63] The OECD guidelines emphasize three groups of cybersecurity principles: (i) 'foundation' principles', (ii) 'social' principles, and (iii) 'security lifecycle' principles. These represent an organizing basis for cybercrime prevention approaches reported by private sector companies.

60 Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks - Towards a Culture of Security, OECD, 25 July 2002 - C(2002)131/FINAL.

61 United Nations General Assembly Resolution 57/239, 31 Jan 2003.

62 See, for example, Council of Europe, Council Resolution on a European approach towards a culture of network and information security, 15723/02, 28 Jan 2003 and APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment, endorsed by the senior officials in November 2005.

63 See http://intgovforum.org/Substantive_1st_IGF/Information.security%20assurance.pdf

Foundation principles – 'Foundation' principles of cybersecurity relate to the importance of organisational risk awareness; accountability for acting on that awareness; and coordination and learning processes to act on incidents.

During information gathering for the Study, private sector respondents emphasized the importance of a holistic approach to security across an enterprise. One company executive commented: '*A lot of insurers ask for very specific things, like 'do you have encryption, do you have firewalls, do you have antivirus software', but what we are really trying to find out is, is security an integral part of the business decisions that a potentially insured company is making, which is very hard to judge, because a lot of companies would do what's minimum necessary in order to protect the data, but they are not making data protection really a top priority item… when you look at security and privacy as separate, standalone functions, separate of everything else that you do, it is not being effective.*'[64] An equipment manufacturer added: '*Companies need a risk management program and policies and practices in place to manage that risk in a way that is transparent…The ability to track your compliance in real-time makes the audit function less expensive.*'[65]

Respondents also focused on the necessity for board-level leadership. An equipment manufacturer said: '*I don't think anybody has really articulated due diligence requirements that you need to follow. In terms of your board of directors, you need to know what you need to worry about, you need to have a visibility to whether or not your enterprise is following recommended practices that constitute due diligence in your country. […] Then, they would not just do financial control; they would do audits of information systems to make sure they are complying with the best practices.*'[66] A medium-sized technology services company noted: '*Most institutions have a handful of people that are extremely aware of the threat and people that are aware of the data the institution collects. The problem is, that there are very few people that have both.*'[67]

Almost all of respondents to the private sector cybercrime questionnaire reported addressing risk awareness through employee training, along with policies and oversight of employee, customer and third party access and use. These measures were universally developed in-house, with implementation cost varying according to the size of the organisation. They include elements such as dissemination of information on latest threats and the limits of technical solutions.[68]

Several respondents commented that training in many companies was not sufficiently effective, although one international services company noted that '*Fundamentals to the practice [of information security and privacy] are increasingly ingrained.*'[69] A mid-sized technology company's security manager said: '*Most threats are actually due to human errors or social engineering. Unsophisticated users can be targeted to get access to the enterprise. That is one of the main challenges that we are working on… If institutions had the right training and policy in place, it would not happen. So prevention is the key.*'[70] A global telecommunications company agreed: '*our biggest challenge is getting all employees to adhere to basic blocking and tackling rules.*'[71]

While threat awareness is growing, some respondents noted that this does not immediately lead to behaviour change. An equipment manufacturer commented: '*I think there's a lot of publicity about threat, but people have to connect threat with their personal responsibility and corporate responsibility.*'[72] A corporate services organisation stated: '*I think there is definitely an awareness of it that there wasn't before amongst industry people, but many people are still uneducated. If you are going to hack a company, you are not*

64 Study cybercrime interview (private sector).
65 Study cybercrime interview (private sector).
66 Study cybercrime interview (private sector).
67 Study cybercrime interview (private sector).
68 Study cybercrime questionnaire (private sector). Q64-67.
69 Study cybercrime interview (private sector).
70 Study cybercrime interview (private sector).
71 Study cybercrime interview (private sector).
72 Study cybercrime interview (private sector).

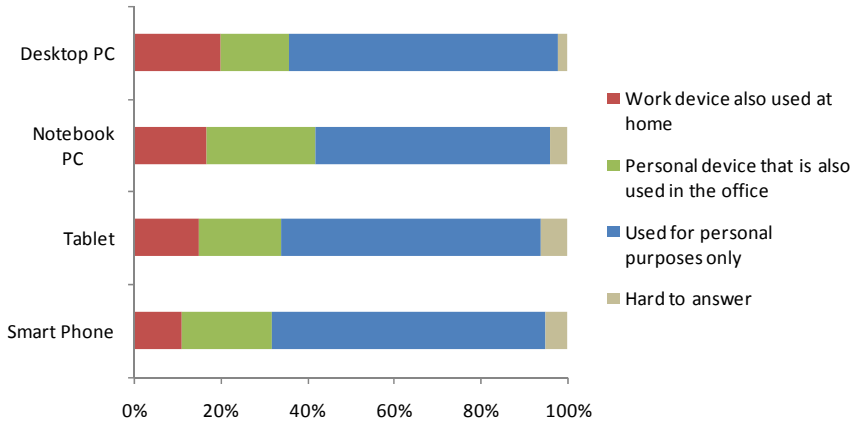
necessarily coming in by the front door. You are coming in via sending a crafted PDF to the head of account when the deputy or the head of account is out for vacation and it's going to get infected from that PDF; then you are going to own their laptop and escalate further into their network, get access to their accounts and payment systems. It is a question of raising awareness of the risks and continually update. There is no silver bullet for any of this.'[73]

Private sector respondents were almost equally split between having one central specialized unit dealing with cybercrime issues, having a number of specialized units (such as for law enforcement liaison and IT security), and having specialized personnel in different work areas. The number of personnel assigned in total increased slowly with company size, varying from 0 to 38 (with one outlier of 120).

Staff commonly dealt with data evidence preservation and advanced internet investigations, with some monitoring emerging cybercrime threats and trends, undertaking law enforcement cooperation, and looking at computer system security approaches. They are mainly trained in-house, with some additional training from the private sector, academia, and non-governmental organisations. In turn, about one-third of respondents provide training on these topics to other organisations, including corporations, government institutions and in some cases international organisations and non-governmental organisations.[74]

Two of the key recent technology changes affecting the information security risk environment are the fast-growing use of cloud computing services, and employee use of their own computing devices (especially smartphones and tablets) to access corporate systems. One survey by a multinational security company of 11,000 internet users in Latin and North America, Europe, the Middle East, Asia and Africa, for example, found that around 15 to 25 per cent of respondents used various personal computing devices at the office.[75]

Figure 8.12: Device usage: personal vs. work



Source: Kaspersky Lab, 2012. Perception and knowledge of IT threats: the consumer's point of view (p.2)

Private sector respondents also identified the increasing impact of cloud computing services on security considerations. One technology consultant respondent noted, for example: '*For the smaller companies using the cloud is probably safer from a cyber standpoint than trying to do-it-yourself with a server in the closet. There are not enough cyber security experts to have one in each company, it obviously would cost way too much money to do that. So, concentrating it at Amazon probably makes a lot of sense from a protection standpoint and also from a response standpoint. It obviously creates targets of opportunity though and it's a lot more fun to breach a large service provider's defences than to breach the corner store's defences*'.[76] Other respondents highlighted the issue of employees using their own devices. A technology consultancy noted: '*I think the accumulation of risk*

[73] Study cybercrime interview (private sector).
[74] Study cybercrime questionnaire (private sector). Q68-73.
[75] Kaspersky Lab. 2012. *Perception and knowledge of IT threats: the consumer's point of view.*
[76] Study cybercrime interview (private sector).

is really coming from bringing your own device. Everyone is bringing very capable devices, they connect into wireless networks, they crossover between social media and email in work and private life. So I think the main threat comes from a lack of cultural ownership of the problem.'[77]

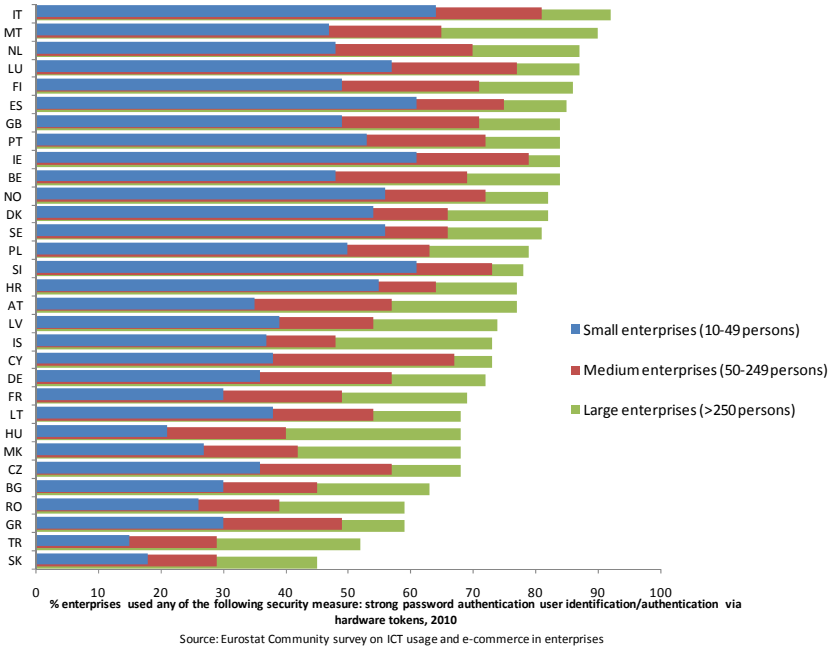
Social principles – The OECD social principles relate to ethical and democratic behaviour by information society participants. This includes awareness of the impact of security breaches on other parties, relevant legislation and regulation, and how employee behaviour lives up to a company's values. It also relates to the compatibility of security practices with societal values such as freedom of expression, privacy, openness and transparency.

Private-sector respondents to the Study were primarily responsible for technical and business decisions related to security and cybercrime, rather than for legal or corporate social responsibility teams. Only one respondent commented in relation to the social principles, noting that: '*In the last few years 'the more data the better' has been most companies' philosophy. You must collect as much data as you possibly can because then we can mine the data, we can use the data and we can do predicted modelling and what's the harm in collecting the data?, with very little thought to what the harm is.*'[78] The respondent further highlighted that this form of behaviour can affect corporate risk assessments, as some corporations tended to underestimate the importance of personal data held by them and the associated risks that this may bring.

Security lifecycle principles – Private sector respondents focused to a larger extent on the OECD security lifecycle principles, which are more operational in nature. These principles are centred on risk evaluation; system design to mitigate identified risks; development of policies, processes and procedures to manage those systems; and continuous review as technology develops.

Surveys of global corporations provide an idea of the extent to which such principles are implemented. Figure 8.13, for example, shows the percentage of European businesses making use of hardware tokens to protect user authentication.[79] The Figure highlights differences in the extent to which small, medium and large enterprises make use of good cybersecurity practice – with smaller enterprises consistently using less secure practices that medium or large enterprises.

Figure 8.13: Strong password authentication and/or user identification and authentication via hardware tokens by size



Source: Eurostat Community survey on ICT usage and e-commerce in enterprises

Two-

77 Study cybercrime interview (private sector).
78 Study cybercrime interview (private sector).
79 Eurostat Community Survey on *ICT usage and e-commerce in Enterprises*.

thirds of private sector respondents to the Study questionnaire stated that their organisations had carried out a cybercrime risk assessment. One major consultancy noted: '*On a twice yearly basis the executive leadership of the company is asked validate priority information security risks, against the Information Security Organization leadership's view. The list of risks under consideration includes, but is not limited to criminal acts.' An equipment manufacturer stated their assessment methods include 'interviews, penetration testing [and] product testing.*'[80]

Several respondents noted a disparity between large, and small and medium size enterprises in risk assessment. One medium-sized technology consultancy stated: *'[small and medium sized enterprises feel] 'we are not prominent; they won't attack us,' which is wrong. It comes from 'we are not worth much, they won't attack us*,' *which is wrong and it comes from 'we don't know what to do' - which is right.*'[81] A global consultancy added: '*For run of the mill criminal activity, banks and big corporations are relatively well set up. Intermediate markets do not have so much in the way of capability; they struggle to respond, to know what to do.*'[82] A small technology consultancy said: '*We do a lot of free educational webinars and we always have had fantastic attendance to our webinars of small and medium-sized businesses. The big businesses will come, too, but the majority is these small and medium businesses coming for the free education. They definitely need the information.*'[83]

Several respondents noted that some smaller companies are still not taking simple steps to protect their systems. A corporate services company commented: '*small/medium size businesses are losing data due to very simple means, not on high-tech means (somebody forgot to change a password – that type of thing)… Most companies are probably not securing their data in rest, just in transit.*'[84] A technology consultancy added: '*The advice we give people primarily are things like: make sure your system is patched, fully up to date; make sure you've got regularly updated antivirus hardware/software; if you don't need Java, Adobe products - take them off; have a stand-alone, isolated computer that you only use for online banking. But you can't defend against a zero day.*'[85] But even at larger companies, a global technology services provider noted: '*Many breaches were and are preventable – all related to basic configurations.*'[86]

Most private sector respondents reported using technical solutions to prevent cybercrime, such as firewalls, digital evidence preservation, and restrictions on specific IP address connections. Many also use identification of certain types of content, measures to prevent copyright/trademark infringement, decryption of encrypted material, and measures against computer misuse. Key elements of these solutions included system supervision and monitoring, intrusion detection and antivirus software. Systems were reported to be mostly developed by the private sector, with some developed in-house, and had a significant annual implementation cost, especially for responding multinational companies.[87]

Respondents disagreed over the threat posed by 'insiders' (employees or other individuals with authorized system access). Two multinational companies noted how large the group of potential 'insiders' had become within their own enterprises: one counted '*300,000 employees worldwide, plus contractors*'[88] and another '*200,000 employees and 50-60,000 vendor or contract employees on our behalf.*'[89] One manufacturer was concerned about '*collusion between insiders and external criminals* [*with*] *insiders interrupting internal systems and manufacturing processes*.'[90] But a security consultancy was less worried, at

80 Study cybercrime questionnaire (private sector). Q49.
81 Study cybercrime interview (private sector).
82 Study cybercrime interview (private sector).
83 *Ibid.*
84 Study cybercrime interview (private sector).
85 *Ibid.*
86 *Ibid.*
87 Study cybercrime questionnaire (private sector). Q60-63.
88 Study cybercrime interview (private sector).
89 Study cybercrime interview (private sector).
90 Study cybercrime interview (private sector).

least for sophisticated companies: '*Yes, there occasionally are some insiders, but we are not seeing insiders that much. The majority of the harm comes from external parties. Certainly banks are very compartmentalized; even if they had an insider, the damage the insider would be able to do is probably fairly limited.*'[91]

Evaluation and review of security policies and procedures is a key part of the OECD security lifecycle principles. A number of private sector respondents noted the importance of real-time monitoring for security incidents. A global consultancy commented: '*We need mechanisms for real-time actionable intelligence and participation. It's a complex problem; there must be a taxonomy, prioritization and determination when incident is critical; everyone must speak the same language, even if they don't share the same goals, and, again, be real-time actionable.*'[92] Another global consultancy added: '*Once they know, they respond well. The situation facing us now is that many companies are not good enough at detection… 12 minutes, not 12 months.*'[93]

Golden Eye v Telefónica

A film producer and owners of copyright in pornographic films took legal action in 2011 to obtain the names and addresses of almost 10,000 ISP customers alleged to have infringed copyright using BitTorrent filesharing software. The High Court in a country in Northern Europe allowed the action for only one of the claimants, commenting that going any further "would be tantamount to the court sanctioning the sale of the Intended Defendants' privacy and data protection rights to the highest bidder." The court was also concerned that the nature of the films at issue could be used to embarrass innocent customers into paying an "unsupportable" standard high "settlement" fee.

The High Court imposed a number of conditions on the letter that could be sent to alleged infringers, due to "the impact … upon ordinary consumers who may not have access to specialized legal advice, who may be innocent of what is alleged against them and who may be embarrassed and/or distressed by being alleged to have been involved in filesharing involving pornography."

Given these safeguards, an appeal from the twelve other claimants was successful. The Court of Appeal granted an order requiring the ISP to disclose details of all of their allegedly infringing customers, enabling further action to be taken against each of them.

A number of private sector respondents highlighted, however, that more could always be done by companies to protect themselves against cyber threats. A global technology services provider said: '*Threats/trends vary, from very simple to the most complex. The key is to know your network and control it in terms of configuration of applications and developing a complex intelligence system…*'[94] Another global technology services provider noted: '*Most customers can't afford to make 24/365 security (info/sec-monitoring) a priority.*'[95] A global consultancy firm suggested that '*some security intelligence work will be outsourced – almost as a clearinghouse for security-decision making information/operations, rather than every major organization running its own global security and intelligence gathering centre.*'[96]

In addition to focusing *inwardly* on its own cybersecurity situation, some global technology companies have taken a *proactive external* approach to investigating and shutting down cyberattacks that threaten consumer trust in their systems. Such initiatives, when carried out with full respect for relevant laws, can complement actions by law enforcement agencies, as well as generate positive publicity and staff morale.

Some of the longest-running series of such legal actions relate to spam e-mails and other unsolicited communications such as instant messages. One of the first large North American ISPs filed dozens of lawsuits against spammers from 1997 onwards, making claims of trespass to chattels,

91 *Ibid.*
92 Study cybercrime interview (private sector).
93 *Ibid.*
94 Study cybercrime interview (private sector).
95 Study cybercrime interview (private sector).
96 *Ibid.*

unjust enrichment and misappropriation, as well as violations of computer crime laws.[97] Subsequently, a group of North American ISPs formed an anti-spam alliance in 2003, taking legal action against dozens of defendants they alleged were responsible for hundreds of millions of unsolicited messages to their customers, using anti-spam and conspiracy laws.[98]

Most recently, one global software company has taken a number of legal actions focusing on botnets, with two main interlocking tactics: seizing control of the command and control mechanisms used to direct machines in a botnet, and seizing machines that contain useful evidence about criminal actions. In a recent case against the Nitol botnet, the company filed suit to take control of 70,000 malicious subdomains. The operator agreed in a settlement to redirect connections to existing and future identified malicious sub-domains to a machine managed by an Eastern Asian CERT. This reduced the ability of the botnet operator to control machines trying to reach such domains, and also provided an opportunity to notify those users and their ISPs that their machines had been compromised.

In the first 16 days after the company took control of the malicious subdomains, they blocked connections from 7.65m unique IP addresses. The operator and company also provided all evidence gathered during the investigation to an Eastern Asian CERT to help with the identification of the original sub-domain operators. Data about infected machines was shared with the Shadow Server Foundation and national CERTs. The company had previously taken similar actions against the Waledac, Rustock, Kelihos and Zeus botnets.[99]

In the Zeus case, the company took more interventionist action. After obtaining a warrant from a federal judge, company lawyers and technical staff seized evidence and deactivated servers hosted in Pennsylvania and Illinois controlling Zeus-related botnets. The company also took control of 800 domains used to coordinate the infected computers. These actions were planned to disrupt the operation of these botnets, as it was not possible to completely shut them down.[100]

A third legal strategy used by the company is to take action against suspected authors of malicious code, with the aim of preventing them creating new malicious code and botnets when their previous efforts are shut down. In 2012 the company filed an amended lawsuit in a district court in North America against a programmer based in Eastern Europe whose code appeared to have been used in the Kelihos botnet. The programmer in question was willing to enter into a confidential settlement agreement.[101]

Similarly, one social media company has taken action against the providers of tools for sending spam, filing suit in 2012 against 'five of the most aggressive tool providers and spammers,' alleging violations of terms of service and inducement of violations by tool users.[102] The company sought an injunction restraining the defendants from creating or offering such software, and requesting damages of at least $700,000.[103]

---

97 Sorkin, D.E., 2001.Technical and Legal Approaches to Unsolicited Electronic Mail. *University of San Francisco Law Review,* 35(2):359-260.

98 McGuire, D., 2004. AOL, E-Mail Companies Sue Spammers. *Washington Post*, 28 October.

99 Microsoft Reaches Settlement with Defendants in Nitol Case. 2012. *The Official Microsoft Blog*, 2 October, available at: http://blogs.technet.com/b/microsoft_blog/archive/2012/10/02/microsoft-reaches-settlement-with-defendants-in-nitol-case.aspx

100 Microsoft and Financial Services Industry Leaders Target Cybercriminal Operations from Zeus Botnets. 2012. *The Official Microsoft Blog*, 25 March, available at: http://blogs.technet.com/b/microsoft_blog/archive/2012/03/25/microsoft-and-financial-services-industry-leaders-target-cybercriminal-operations-from-zeus-botnets.aspx

101 Microsoft Reaches Settlement with Second Kelihos Defendant. 2012. *The Official Microsoft Blog*, 19 October, available at: http://blogs.technet.com/b/microsoft_blog/archive/2012/10/19/microsoft-reaches-settlement-with-second-kelihos-defendant.aspx

102 Shutting down spammers. 2012. *Twitter Blog*, 5 April, available at: http://blog.twitter.com/2012/04/shutting-down-spammers.html

103 *Twitter Inc. v. Skootle Corporation*. 2012. US District Court, Northern District of California, case no. CV 12-01721, 5 April.

Two other large service providers have also taken action against advertisers misusing their services. One large search engine, for example, obtained a permanent injunction against a company that had been advertising fraudulent money transfer schemes,[104] and sued advertisers deliberately breaching its terms of service.[105] A large social networking service similarly filed suit against a company that designed pages and links that tricked users into providing personal information, into signing up for expensive subscription services, and into 'liking' a website page, and hence sharing it with their friends.[106] The defendant settled with the company.

A number of internet security companies further gather detailed data on the prevalence of malicious software and botnets, which are published in regular reports and shared with corporate and law enforcement partners. Several companies publish quarterly threat reports, which contain data on levels of machine infections (including mobile devices), database breaches, attacks such as phishing, and specific cybercrime activities such as ransom demands and crimeware tools.[107] One Eastern European security company has published data gathered on groups and individuals involved in cybercrime in the region,[108] while another security company recently published a report comparing the profiles of East Asian and Eastern European cybercrime attackers.[109] Many telecommunications companies share data on traffic patterns and attacks seen on their networks. One such observatory, for example, produces a real-time global threat map with daily briefs on significant events.[110]

A more recent phenomenon has been the consideration of the use of intelligence gathering by companies to respond to attacks. Several private sector organizations assist companies to profile adversaries and their motivations for attacks. This information enables better technical defences, fine-tuned legal action, deception (such as planting false information on companies' own networks), and making attacks more resource-intensive.[111] Some companies have considered 'hacking back' against attackers, but it is presently unclear how far this would be legally or technically feasible.[112]

Overall, the picture reported by private sector respondents regarding cybercrime prevention is mixed. Larger companies, particularly in the financial services industry, have sophisticated prevention strategies, including using specific security technologies such as hardware authentication tokens. Security companies actively monitor and publish regular reports on the emergence of new threats, while some large technology firms have taken proactive legal action to shut down botnets, spammers and fraudsters. However, smaller companies are not so well-positioned, with some not taking basic precautions or having any realistic picture of security risks.

---

104 Fighting fraud online: taking 'Google Money' scammers to court. 2009. *Google Official Blog*, 8 December, available at: http://googleblog.blogspot.co.uk/2009/12/fighting-fraud-online-taking-google.html

105 Taking rogue pharmacies to court. 2010. *Google Official Blog*, 22 September, available at: http://googleblog.blogspot.co.uk/2010/09/taking-rogue-pharmacies-to-court.html

106 Facebook, Washington State AG Target Clickjackers. 2012. *Facebook Security Notes*, 26 January, available at: http://www.facebook.com/notes/facebook-security/facebook-washington-state-ag-target-clickjackers/10150494427000766

107 See, for example, *McAfee Threats Report: Third Quarter 2012*, available at: http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2012.pdf

108 Group-IB. 2012. *State and Trends of the 'Russian' Digital Crime Market 2011*, available at: http://group-ib.com/images/media/Group-IB_Report_2011_ENG.pdf

109 Trend Micro. 2012. *Peter the Great Versus Sun Tzu*, available at: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/spotlight-articles/op_kellermann_peter-the-great-vs-sun-tzu.pdf

110 See http://atlas.arbor.net/about/

111 Higgins, K.J., 2012. Turning Tables: ID'ing The Hacker Behind The Keyboard. *Dark Reading*, 2 October, available at: http://www.darkreading.com/threat-intelligence/167901121/security/attacks-breaches/240008322/turning-tables-id-ing-the-hacker-behind-the-keyboard.html

112 Simonite, T., 2012. Fighting Hackers without Sinking to Their Level. *MIT Technology Review*, 26 July, available at: http://www.technologyreview.com/news/428584/fighting-hackers-without-sinking-to-their-level/

Cybercrime prevention by internet service and hosting providers

Internet service providers and hosting providers are uniquely placed within the internet infrastructure. As described in Chapter One (Global connectivity), service providers own or lease high capacity fibre optic and cable transport, as well as other core infrastructure such as servers, switches and routers, and (in the case of mobile network operators) radio cells, that enable content to be hosted and delivered, and desktop and handheld devices to connect to the internet. That service providers should have some role in cybercrime prevention is, at the same time, both 'obvious', but yet nuanced and complex – engaging issues such as service provider liability and responsibility for internet content. In order to consider service provider cybercrime prevention possibilities further, it is first necessary to briefly examine a number of technical aspects.

ISPs connect users to the internet by transmitting data between users and devices such as web, e-mail, and VOIP servers. ISPs can potentially analyse some of this traffic, unless the user encrypts data using a Virtual Private Network, proxy server, or functionality built in to communications software. The customer data that ISPs can access includes the *content* of communications – unencrypted text and images on websites or in emails – and *contextual* data such as which services are visited, the source and destination of emails, what times different services are used, and how long the user spends on different services, even if basic website encryption is being used. In general, content data can only be observed at the moment that it is sent, and then only by explicitly monitoring the user's connection and storing the data using specialist equipment. A notable exception is when an ISP is running a service such as an e-mail server, which stores messages for longer periods of time.

An individual will often use several ISPs as they access the internet from different locations. A home user's service provider is often different from their mobile provider. Their Internet access at work may use a third provider, and connection to a wireless network in a local café will involve yet another ISP handling the connection. The information about the activities of one individual may therefore be spread over many different providers.

Internet hosting providers have control over the systems on which websites and other services are run. As with the relationship between ISPs and their customers, hosting companies have a privileged view of all traffic passing to and from their customers' hosted services. They therefore have the technical possibility to disable or block illegal use of such services. Hosting companies typically place restrictions on the nature of services that can be hosted with them through service agreements, which often cover well-known abusive behaviour such as the sending of large volumes of spam or abusive email, hosting illegal content, or being used to violate copyright.

Service providers can play a role in cybercrime prevention within two main areas: (i) through the storage of user data that can then be accessed and used by law enforcement in cybercrime investigations; and (ii) through active 'filtering' of internet communications or content with a view to preventing cybercrime acts in the first place. This section examines the technical and regulatory aspects of each of these areas.

Data storage – Due to the volume of traffic passing across their networks, it is infeasible for ISPs to keep a complete record of all traffic. Some countries have implemented sophisticated internet surveillance systems, but the technological limitations of gathering and analysing huge volumes of data can be challenging. Logging of less detailed information (such as IP addresses assigned to individual users at particular times) can occur over long periods of time. ISPs generally have the ability to undertake targeted 'real-time' monitoring of data, and (as discussed in Chapter

Four (Law enforcement and investigations)), 'lawful intercept' rules in many States require ISPs to have the capability to conduct targeted real-time monitoring of connections of an individual or premises.

Data protection – Storage and processing of data by ISPs is subject, in many countries, to data protection laws that impose requirements on the protection and use of personal information.[113] In 1990 the UN General Assembly adopted Guidelines for the Regulation of Computerized Personal Data Files.[114] These contain ten principles, including fairness, accuracy, and purpose specification, and apply to '*all public and private computerized files*'. A security principle states that files should be protected against '*human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses.*'A 2012 review of data protection laws found comprehensive laws in 89 countries, with draft bills in a further 10 countries.[115]

Some regional data protection frameworks – such as the EU legal framework – include specific rules on data protection in the electronic communications sector.[116] Under this framework, publicly available communications services must take '*appropriate technical and organisational measures to safeguard security…if necessary in conjunction with the provider of the public communications network with respect to network security.*' Traffic data about users may only be processed for specific purposes, and should be erased or anonymized when no longer needed (although see the following subsection on data retention.) EU member states may restrict some of these rights when required to safeguard purposes including '*public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system.*'

During information gathering for the Study, the majority of responding countries indicated some constitutional and/or statutory provisions to protect the privacy of personal data. A typical purpose described for data protection laws was to *'govern the collection, use and disclosure of personal information in manner that recognizes both the individual's right to privacy, and the information needs of an organization.'*[117] With respect to the contribution of ISPs to cybercrime prevention, data protection laws can have a number of effects. Data processing restrictions should not in general (at least where sufficient legal exceptions exist) prevent lawful access to ISP customer data by law enforcement for investigative purposes. A typical exception reported was that *'a non-law enforcement entity (including a company) that holds personal information is permitted to disclose the information to a law enforcement agency without breaching the Privacy Act where it is 'reasonably necessary' for the enforcement of the criminal law.'*[118]

However, data protection obligations that require personal data to be deleted when no longer required for the purposes for which it was collected, may impact on police cybercrime investigations. As noted in Chapter Four (Law enforcement and investigations), for example, a

---

113 The OECD and Council of Europe agreed similar sets of principles for such personal data processing at the beginning of the 1980s (See OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980; Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS no. 108, 1981.) Other regional organizations have since adopted data protection rules, including notably the Asia-Pacific Economic Cooperation, the Economic Community for West African States, and Organization of American States (See APEC Privacy Framework, 2005 Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS, 2010, and General Assembly Resolution 2661 on Access to Public Information and Protection of Personal Data, 2004). The European Union has developed a comprehensive set of data protection rules, with a right to data protection being part of the Union's Charter of Fundamental Rights (along with a broader right to privacy, including of communications). The Directive on Data Protection contains detailed rules which apply to public and private sector organizations including ISPs (See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L 281 , 23/11/1995 p.31 -50.)

114 United Nations General Assembly, Resolution 45/95, 14 December 1990.

115 Greenleaf, G., 2012. Global Data Privacy Laws: 89 Countries, and Accelerating. *Privacy Laws & Business International Report*, Issue 115, Special Supplement.

116 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. OJ L 201, 31.7.2002, pp.37–47.

117 Study cybercrime questionnaire. Q22.

118 Study cybercrime questionnaire. Q24.

number of law enforcement authorities reported challenges with short ISP data retention times and this may be due, in some circumstances, to the effect of data protection laws. In addition, data protection laws – as for all organizations and individuals that process personal data – contribute to cybercrime prevention from the ISP perspective, by providing data processing standards that help to ensure the safety and integrity of user data.

Data retention – The combined effect of data protection laws and the financial implications of storing large amounts of data, mean that ISPs do not have indefinite data retention times. With a view to assisting law enforcement investigations, a number of countries have introduced exceptions to data protection laws in order to require ISPs to store specific types of data about customer online activities for periods of time (such as a year), during which it can be accessed by investigators with judicial or administrative authorisation.

The most widely applicable of such laws is the EU Directive on Data Retention.[119] EU member states must require ISPs to store data they generate that is necessary to trace and identify the source of a communication; identify the destination, type and timing of a communication; and identify users' communication equipment. This data must be stored for a period between six months and two years. A number of national courts have questioned the proportionality and impact on privacy of these requirements.[120]

A small number of other States have considered or implemented retention laws. One country in Oceania, for example, has proposed an EU-style system, which has been under consideration by a parliamentary joint committee.[121] Another country in Southern Asia has legislation that enables the government to define requirements for intermediaries to retain electronic records, but such rules have only been defined for cyber cafes.[122] In contrast, the Supreme Court of one country in South America annulled a data retention law in 2009 on the grounds of interference with the privacy rights of the individual.[123]

The UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism has expressed concern that '*in many countries, data retention laws have been adopted without any legal safeguards over the access to this information being established or without the fact that new technological developments are blurring the difference between content and communications data being considered. While constitutional provisions tend to require safeguards on access to communications content, the protection of transaction logs is more limited. While this information may be integral to investigations, it may also be just as privacy-sensitive as the content of communications transactions.*'[124] Thus, while data retention laws may represent a pragmatic approach to ensuring that ISPs are able to play a greater role in cybercrime prevention through enhanced law enforcement cooperation, it is important that such laws are implemented with due procedural safeguards and privacy protections.

Data breach notification – Finally, ISP storage of customer data may be affected by 'mandatory reporting of security breach' requirements. Mandatory reporting of security breaches to affected parties and to regulators, especially when personal data is disclosed, has gained widespread support

---

119 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ L 105/54, 13 April 2006.

120 Brown, I. 2010. Communications Data Retention in an Evolving Internet. *International Journal of Law and Information Technology* 19(2):95-109.

121 Australian Government Attorney General's Department, 2012. *Equipping Australia against emerging and evolving threats: A Discussion Paper to accompany consideration by the Parliamentary Joint Committee on Intelligence and Security of a package of national security ideas comprising proposals for telecommunications interception reform, telecommunications sector security reform and Australian intelligence community legislation reform.*

122 Privacy International. 2012. *Country report: India, Privacy in the Developing World*, available at: https://www.privacyinternational.org/reports/india-0

123 Halabi, Ernesto c/ P.E.N. - ley 25.873 (Acción de clase, Argentina).

124 United Nations Human Rights Council, Thirteenth session, A/HRC/13/37, 28 December 2009, p.16.

in a number of countries. Notification is intended to enable victims of breaches to take measures to reduce the security impact (such as changing passwords or PINs, or asking for payment cards to be reissued); to increase the competitive pressure on businesses to improve their security; and to support the work of regulators responsible for data protection and critical infrastructure protection.

Data breach notification laws exist at the sub-national level in countries in North America.[125] The European Union also requires public communication networks and services to report significant breaches to national authorities[126] and to adversely affected individuals.[127] It is currently considering the extension of this requirement to all organisations that process personal data.[128] Notification requirements or guidelines have also been introduced by countries in Oceania, and South Eastern and Southern Asia.[129]

While data breach notifications can represent an important element of information security regimes – including as applicable to ISPs - such laws must ensure that they define the term 'security breach' with care, and are used in conjunction with a range of other measures, including effective data protection laws.

Filtering of internet content – In addition to crime prevention opportunities related to data storage, ISPs may also play a role in preventing cybercrime through active review of the internet communications and data that they carry. One key concept in this respect is the possibility of internet 'filtering' by ISPs.

Filtering of internet connections occurs, at some level, on almost all networks. The most basic level of filtering is employed to improve network performance and security by dropping invalid and otherwise corrupted data. ISPs may also have the technical ability to filter for specific malicious or illegal content. Many ISPs implement basic spam filtering for their users' email accounts, for example, and may also protect against well-known malicious traffic coming from viruses or hacking attempts, by refusing to pass on traffic identified as such.

Spam and botnets – Spam filtering is a major concern of all email providers due to the high volume of spam messages sent and received every day. The means by which spam is filtered are varied and complex, including analysis of the origin of emails to identify known sources of spam, as well as textual analysis to identify common phrases and patterns of content in the messages. Messages identified as spam are sometimes dropped entirely, or delivered to user 'spam folders'. In addition to filtering of spam, ISPs may also play a role in combating malicious traffic, such as that generated by botnets.

When ISPs are notified, or identify from internet traffic patterns, that a machine in their network appears to be part of a botnet or is otherwise infected with malicious software, one option is to block some or all of the traffic from that address, while notifying the customer of steps they can take to remove the malicious software. These notifications can come from security companies monitoring botnets, using techniques such as 'honeypot' machines that deliberately attract malicious software. ISPs can also take steps to proactively identify compromised machines by monitoring

---

125 National Conference of State Legislatures, 2012. State Security Breach Notification Laws, at http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx

126 Article 13a of Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (OJ L 108, 24.4.2002, pp.33–50).

127 Article 4 of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ L 201 , 31/07/2002 pp.37-47).

128 Articles 31 and 32 of the Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. COM(2012) 11 final.

129 Maurushat, A., 2009. Data Breach Notification Law across the World from California to Australia. *Privacy Law and Business International*. UNSW Law Research Paper No. 2009-11.

traffic for known signatures, although some amount of targeting is required to make this effective. A review from the European Network and Information Security Agency concluded that: '*Identifying botnet traffic among benign, regular traffic is like searching for a needle in 100 million haystacks.*' As noted above and in Chapter Five (Law enforcement and investigations), general traffic monitoring may also, in some circumstances, risk conflict with data protection and privacy laws.[130]

Content filtering – As discussed below in the context of ISP *liability*, laws in some countries require ISPs to block access to illegal content such as child pornography. There are various ways in which ISP can do this, with different methods making tradeoffs between speed, cost, effectiveness and accuracy. Using *DNS Filtering*, ISPs can control the answers given to users by their DNS server, thereby restricting access to a domain, such as 'google.com', but not a specific page or set of search results. This is easy to bypass as users can simply use alternative DNS servers that will give genuine results. *IP Header Filtering* can be used to block individual computers based on their addresses or even partially to block specific services such as web or email. As many websites may be running on a single internet server, it can affect unrelated websites – sometimes in very large numbers. *Deep Packet Inspection* can be used to examine the main body of internet traffic. This allows extremely flexible filtering, but requires expensive hardware on high-speed ISP links, and can slow all user connections.

In practice, many filtering regimes employ a combination of these approaches, forming a hybrid filter. Often, simpler filters, such as those based on DNS, are used to identify traffic to be redirected to more complex filters. This hybrid approach allows sophisticated filtering with greatly reduced resources.

Another possible ISP response to illicit content is to slow down traffic rather than blocking it altogether. This approach can be used to make a service sufficiently inconvenient that users avoid it. Examples of this include the slowing of encrypted web connections, to force users onto unencrypted and thus inspectable versions of websites, and the practice of ISP 'throttling' of filesharing traffic such as BitTorrent.

Possibilities for filtering or blocking of content, including with the aim of cybercrime prevention, have raised a number of human rights concerns. The Human Rights Council has emphasized, for example, the importance of internet access to freedom of expression and other human rights. A resolution adopted at its 20th session '*Affirms that the same rights that people have offline must also be protected online, in particular freedom of expression,*' and '*Calls upon all States to promote and facilitate access to the Internet.*' [131] The Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, has similarly called the internet '*an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress… facilitating access to the Internet for all individuals, with as little restriction to online content as possible, should be a priority for all States.*'[132]

Intermediary liability – Internet content filtering is closely linked with the possibility of imposition of service provider *liability* for content. ISPs typically have limited liability as 'mere conduits' of data. However, as discussed below, particularly in the context of internet hosting, modification of transmitted content can increase liability in some legal systems, as can actual or

130 Hogben, G., (ed.) 2011. *Botnets: Detection, Measurement, Disinfection & Defence.* ENISA, pp.73-74.
131 A/HRC/20/L.13, 29 June 2012.
132 A/HRC/17/27, 16 May 2011.

constructive knowledge of an illegal activity. Expeditious action after notification, on the other hand, tends to reduce liability.[133]

Many legal systems include notions of secondary liability, where one party that has contributed to wrongful actions of another may be partly liable for harm that results. As the internet became widely used in the mid-1990s, concerns were raised about the impact on the emerging digital economy of uncertainty about liability for ISPs and hosts of online content. In response, a number of countries passed 'horizontal' legislation limiting such liability across *multiple* areas of law. These provisions generally protect intermediaries from responsibility for transmitting or hosting third-party content, so long as they meet certain conditions, particularly the removal of specific content when given notice. A number of states have also introduced 'vertical' regulation regarding secondary liability in *specific* areas, such as protection of children, personal data, counterfeiting, defamation, payment fraud, domain names, and online gambling.[134]

Countries in North America and Europe introduced two of the earliest horizontal regimes, with a number of common elements. Legislation in one country in North America, for example, contains a broad limit on service provider liability, except related to communications privacy and intellectual property law and federal criminal statutes. It states that '*No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider… No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.*'[135]

The EU's Directive on e-Commerce[136] similarly protects ISPs and other '*intermediary service providers*' that provide goods or services online. It excludes several areas of law, including taxation, data protection, cartels, and gambling. For ISPs acting as a '*mere conduit*' of transmissions, EU states must '*ensure that the service provider is not liable for the information transmitted*'. Services caching information to enable more efficient onward transmission are similarly protected, provided that they comply with rules concerning access to and updating of that information, and remove or disable access to information after notice that the source material has been removed. Content hosts must expeditiously remove or disable access to infringing information when given actual or constructive knowledge of its existence.

EU states cannot impose a general obligation on service providers to monitor information they transmit or store, or '*actively to seek facts or circumstances indicating illegal activity*.' However, courts or administrative authorities may require providers '*to terminate or prevent an infringement'*, or establish '*procedures governing the removal or disabling of access to information*.'[137]

Of the domain-specific liability regimes, copyright has received the greatest attention. In one country in North America, secondary liability for copyright infringement is specifically limited by legislation.[138] This creates safe harbours for service providers providing transitory digital network communications, system caching, content hosting, and information location tools. It generally requires a notice and takedown system, a policy for terminating accounts of repeat infringers, and accommodation of standards-based technical measures for controlling access to works. Rights holders may file suit for an injunction blocking access to infringing material, terminating subscriber

133 OECD, 2011. *The role of Internet intermediaries in advancing public policy objectives*. DSTI/ICCP(2010)11/FINAL, pp.13, 16-17, 24.
134 *Ibid.*
135 47 USC § 230 - Protection for private blocking and screening of offensive material.
136 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market. OJ L 178, 17 July 2000, pp.1–16.
137 *Ibid.*
138 17 USC § 512 - Limitations on liability relating to material online.

accounts, or other '*comparably effective*' relief that is '*least burdensome*' to the service provider for that purpose.

There has also been broad international discussion related to responsibilities of intermediaries to take action against child pornography. A number of countries in Southern Europe, Eastern and Western Asia, and Oceania require ISPs to block customer access to sites reported to contain such material.[139] Interpol maintains a worldwide list of website addresses containing material of a 'severe nature', which ISPs in some countries have been instructed to block under telecommunications laws. The European Parliament, however, rejected a legislative proposal from the European Commission that would have imposed mandatory blocking on ISPs across the EU, leaving the decision to individual member states.[140]

Overall, internet service providers and hosting providers can play a key role in cybercrime prevention due to their position of connecting individuals and organisations to the Internet. They may retain logs that can be used to investigate criminal activity; help customers to identify compromised computers; block some kinds of illegal content such as spam; and in general support a secure communications environment for their customers. Data protection laws in many countries require ISPs to protect customer data, and investigative powers need to ensure police access to this data is proportionate. Freedom of expression rules must also be taken into account in legislation that provides for interference in the free flow of information across the Internet. Protection from liability for ISPs and other intermediaries has been a key factor in the rapid growth of online services, while placing certain responsibilities on ISPs, such as action when notice is provided of copyright infringement and other infractions.

The involvement of academia in cybercrime prevention

Academic institutions and intergovernmental organizations are important stakeholders in the prevention and combating of cybercrime. Such institutions may contribute, in particular, through knowledge development and sharing; legislation and policy development; the development of technology and technical standards; the delivery of technical assistance; and cooperation with law enforcement authorities.

Knowledge development and sharing – In response to governmental and industry demands for cybersecurity professionals and workforce development needs, academic institutions have established specialized educational programs, curricula and training centres to consolidate knowledge and research, and increase synergies in knowledge across domains and disciplines. A growing number of universities offer degrees, certificates, and professional education in cybersecurity and cybercrime related topics to promote '*educating and training young adults and future professionals about safe computing practices and technical matters*'[141]. Universities also promote applied learning and the development of social networks against cybercrime through the organization of workshops and conferences. These provide opportunities for the exchange of information and advice on preventative and response measures, the cultivation of informal cooperation, and, at times, mechanisms for specific act reporting and development of technical solutions.

Academic contributors to cybercrime control efforts come from a wide range of disciplines, including computer science and engineering, law, criminology and sociology. The past two decades has seen a significant growth in the number of academic journals dedicated to issues related to

139 See OECD2011. *The role of Internet intermediaries in advancing public policy objectives*. DSTI/ICCP(2010)11/FINAL, p.46

140 Article 25(2) of Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA (OJ L 335 , 17.12.2011)

141 Study cybercrime questionnaire (IGO and academia). Q70.

cyberspace, cybersecurity, and cybercrime.[142] Awareness and research on related issues has resulted in an increasing number of technical reports, research and peer-reviewed publications, agency data analysis, and unpublished proprietary research.

Legislation and policy development – University specialists provide a significant contribution to the development and amendment of legislation and policy. At the national, regional, and international level, academics provide legal advice and draft legislation on a range of topics, including criminalization, confidentiality and privacy, constitutional and legal protections. Such advice is delivered through a range of mechanisms, including participation in advisory groups and task forces, institutional and individual contracts, and through technical assistance programs. One academic respondent, for example, noted that dedicated cyber research centres frequently act as coordinators: *'of activities of specialized researchers within different work areas related to cybercrime (legal, criminological, technical expertise)'.*

Technology and technical standards –Universities undertake pure and applied scientific research on computer technology, either in the context of academic-private sector and/or government cooperation, internal or external sponsored research, or as means to secure the university network. Universities may also contribute to computer forensics, evidentiary analyses and agency data analyses. In addition to institutional and individual research, universities also represent important partners and facilitators of cooperation, through participation in professional organizations and standards organizations, as well as technical working groups. A few national cybersecurity strategies explicitly mention the role of universities in efforts to secure cyberspace.[143]

Technical assistance – University technical assistance programs in the area of cybercrime are often designed for and delivered to national and international law enforcement, criminal justice and national security agencies. Universities also deliver technical assistance to corporations, small and medium business enterprises, and to other academic institutions. These programs cover a range of substantive areas related to investigative techniques, evidence preservation and digital forensics; malware analysis content analysis (as distinct from forensics); policy, governance, and compliance; drafting and amendment of legislation and, prosecution and trial support.[144] In conjunction with knowledge development and technical assistance activities, a few universities have developed special educational programs, for example, in cybercrime investigations and digital forensics, to which police and governmental authorities formally second their employees as students.

Cooperation with law enforcement – Law enforcement authorities can have incentives to cooperate with universities, due to university-based cybercrime and cybersecurity expertise. University respondents cooperate with law enforcement in knowledge development, technical standards, and technical assistance, although many academic respondents also reported no direct interaction with law enforcement.[145] Academic respondents frequently highlighted that resource availability to expand such educational efforts and communication is a concern. One respondent noted, for example, that: '*There are no general institutionalized grounds for cooperation - state agencies have*

---

142 Including, for example, *Cyberpsychology, Journal of Psychosocial Research on Cyberspace; Cyberspace and Intellectual Property; Digital Evidence and Electronic Signature Law Review; Journal of Law & Cyber Warfare; International Journal of Cyber Behavior, Psychology, and Learning; International Journal of Cyber Society and Education; International Journal of Cyber Ethics in Education; International Journal of Cyber Warfare and Terrorism; International Journal of Cybercriminology; International Journal of Electronic Security and Digital Forensics; and Journal of International Commercial Law and Technology.*

143 Australia, Czech Republic, Estonia, Germany, India, Japan, Netherlands, New Zealand, Nigeria, United Kingdom and United States are among the countries whose national strategies specifically refer to academia or universities as critical stakeholders and partners in their national cybersecurity strategies.

144 Other topics include international cooperation, transnational organized crime, general telecommunications and technology, and prevention issues.

145 This may be due to the responder's position and knowledge of University risk management, systems and operations. A majority of academic respondents were faculty members, as opposed to University IT, risk management or security personnel.

neither any standards nor a budget for cooperation with universities. Thus, all existing contacts and cooperation are informal'. '*Funding, staff size and availability of specialized academic personnel*'[146] to assist with public safety efforts were seen as necessary to improve outcomes, particularly '*increased funding for research into forensic tools and analysis, and training and skilled personnel*'.[147] Despite the need for '*More resources and openness in law enforcement, and more applied research in academia*',[148] significant potential exists for expanded cooperation with government institutions and law enforcement authorities.

146 Study cybercrime questionnaire (IGO and academia). Q70.
147 Study cybercrime questionnaire (IGO and academia). Q70.
148 Study cybercrime questionnaire (IGO and academia). Q70.

Page left intentionally blank

ANNEX ONE: ACT DESCRIPTIONS

Acts against the confidentiality, integrity and availability of computer data and systems	
Illegal access to a computer system	Refers to acts involving entry into parts or the whole of a computer system without authorization or justification. This is the case, for example, if a perpetrator circumvents a firewall and enters the computer system of (for instance) a bank. This may also be the case if a user continues to remain connected to a computer system beyond his or her authorized time, such as when a perpetrator books server capacities for a certain period of time but continues to use them after the period has expired. Some national approaches require that the perpetrator circumvents protection measures or acts with specific intent.
Illegal access, interception or acquisition of computer data	Refers to acts involving gaining access to computer data without authorization or justification, including obtaining data during a transmission process that is not intended to be public, as well as obtaining computer data (such as by copying data) without authorization. This is the case, for example, if a perpetrator illegally accesses a computer database, records transmissions without right within a wireless network, or if a perpetrator, who is working for a particular company, copies files to take with him without authorization. Some national approaches require that the relevant data was protected against unauthorized access. Some national approaches also include the interception of electromagnetic emissions that may not be categorized as computer data. Industrial or corporate espionage may often involve the act of illegal access, interception or acquisition of computer data.
Illegal data interference or system interference	Refers to acts hindering the functioning of a computer system, as well as to acts involving damage, deletion, deterioration, alteration or suppression of computer data without authorization or justification. This is the case, for example, if a perpetrator submits so many requests to a computer system that it can no longer respond to legitimate requests (a so-called 'denial-of-service attack'), deletes computer program files necessary for the functioning of an internet server, or alters records in a computer database. Some national approaches cover only data-related acts whereas others also cover hardware manipulations. 'Hacking' into computer systems associated with critical infrastructure (such as water or electricity supply systems) may result in illegal data interference or system damage.
Production, distribution, or possession of computer misuse tools	Refers to acts involving the development or distribution of hardware or software solutions that can be used to carry out computer or internet-related offences. This is the case, for example, if a perpetrator develops a software tool to automate denial-of-service attacks. In order to avoid interference with the legitimate use of such tools (such as by security experts), some national approaches require that the tool is exclusively designed for illegal purposes, or that a perpetrator acts with the intention to use the tool to commit a crime.
Breach of privacy or data protection measures	Refers to acts involving the use of a computer system to process, disseminate, obtain, or access personal information in violation of data protection provisions. This is the case, for example, if a perpetrator operates an e-commerce business and discloses personal information from his customer database that he was required to keep confidential.
Computer-related fraud or forgery	Refers to acts involving interference with or illegal accesses to a computer system or data with the intent of deceitfully or dishonestly obtaining money, other economic benefit or evading a liability, as well as to acts involving interference with a computer system or data in way that results in the creation of inauthentic computer data. This is the case, for example, if a perpetrator modifies the software used by a bank to redirect money transfer processes to his own account, or if a perpetrator modifies an authentic email from a financial institution with an underlying intent to defraud. Sending many such messages in an attempt to obtain personal information or to defraud is also referred to as 'phishing.' With respect to computer-related forgery, some national approaches require that the original computer data relate to documentation intended to create binding legal obligations. Others require only that a perpetrator intends the resultant modified version to be considered as or acted upon with respect to legal obligations.
Computer-related identity offences	Refers to acts involving the transfer, possession, or use, of means of identification of another person stored in computer data, without right, with the intent to commit, aid or abet any unlawful criminal activity. This is the case, for example, if a perpetrator, without right, obtains driving licence information from a computer system and either sells such data or uses it to hide his true identity when committing a crime. Some national approaches limit the application of such provisions to certain identification instruments.
Computer-related	Refers to acts involving the copying of material stored in computer data or generates computer

copyright and trademark offences	data in violation of copyright or trademark protections. This can be the case, for example, if a perpetrator distributes a song protected by copyright through a file-sharing system without the license of the copyright owner.
Sending or controlling sending of spam	Refers to acts involving the use of a computer system to send out messages to a large number of recipients without authorization or request. In order to avoid an interference with regular business to customer communications, some national approaches require that a perpetrator provides false header information in such messages.
Computer-related acts causing personal harm	Refers to acts involving the use of a computer system to harass, bully, threaten, stalk, or to cause fear in or intimidation of an individual. This is the case, for example, if a perpetrator sends insulting, threatening, offensive or abusive messages or images (also referred to as 'trolling'), or uses a computer system to track, stalk, or otherwise monitor or interfere with an individual's emotional or physical well-being. Acts solely constituting defamation are excluded from this category.
Computer-related acts involving racism or xenophobia	Refers to acts involving the use of a computer system to distribute or to make available racist and xenophobic material, or to threaten or insult an individual or group of persons for racist or xenophobic reasons. Racist and xenophobic material means any written material, image or other representation of ideas or theories which advocates, promotes or incites hatred, discrimination or violence against any individual or group of persons, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.
Computer-related production, distribution, or possession of child pornography	Refers to acts involving the use of a computer system to produce, create, distribute, access or view, receive, store or possess any representation, by whatever means, of any real or fictional person under 18 years of age, or appearing to be under 18 years of age, engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes. This is the case, for example, if a perpetrator downloads a digital picture showing the sexual abuse of a child.
Computer-related solicitation or 'grooming' of children	Refers to acts involving the use of a computer system, to propose to a child who has not reached the age of sexual consent to meet, for the purpose of committing a sex-related crime. This is the case, for example, if a perpetrator enters an internet chat with a child, pretends that he is also a child, and proposes to the child to meet, with the intention of abusing the child. This conduct may also be termed 'grooming'. Some national approaches may limit the offence to solicitation that is followed by a material act leading to a meeting.
Computer-related acts in support of terrorism offences	Refers to acts involving the use of a computer system in support of terrorism offences. This includes the use of a computer system to communicate a message to the public, with the intent to incite the commission of a terrorist offence or offences, where such conduct, whether or not directly advocating terrorist offences, presents a danger that one or more such offences may be committed (computer-related 'incitement to terrorism'). This also includes the use of a computer system to provide or collect funds with the intention that they should be used, or in the knowledge that they are to be used, in full or in part, in order to commit a terrorist offence or offences (computer-related 'terrorist financing offences'). This also includes the use of a computer system for the planning, research, preparation, or organization of a terrorist offence or offences (computer-related 'terrorist planning offences'). A terrorist offence means any act established in accordance with the universal legal instruments against terrorism, or otherwise intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities of a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or abstain from doing any act.

ANNEX TWO: MEASURING CYBERCRIME

Police-recorded crime statistics

Police-recorded crime statistics are usually considered the administrative statistics closest to actual crime events.[1] Nonetheless, as is well known, police-recorded crime statistics capture only those events that come to the attention of the police. As a result they typically conceal (an often significant) 'dark figure' of crime.[2]

For cybercrime events, the difference between victimization and police-recorded crime can be many orders of magnitude. Online consumer credit card fraud victimization reported in population-based surveys, for example, may alone be more than 80 times greater than total police-recorded computer-related fraud and forgery in the same country.[3] According to one population-based survey of almost 20,000 individual internet users in 24 countries, only 21 per cent of respondents who said that they had been a victim of any cybercrime act indicated that they had reported the act to the police.[4]

A further difficulty with police-recorded crime statistics is the development of a cross-nationally comparable approach to identifying the involvement of computer systems or data in a particular act. National police incident-based reporting systems have various ways of recording an act as 'cybercrime.' Record fields may use indicators such as '*whether the computer was the object of the crime*' or '*where the offender used computer equipment to perpetrate the crime*.'[5] Other approaches are based simply on articles of national criminal legislation, and thus only cover a limited number of cybercrime acts, such as 'computer misuse.'[6] This results in police statistics that range from the proportion of 'conventional' acts in which a computer was the tool or object, to statistics only for technology-specific offences.[7] In the former case, it can be challenging to understand the threshold for, and meaning of, the use of computer equipment 'to perpetrate' a particular crime.[8] In the latter case, cross-national comparisons may only be made where national legislation – and corresponding categories used for statistical purposes – are equivalent. In order to understand, for example, whether police statistics for '*unauthorized use of a computer*' in one country can be compared with statistics for '*illegal access to a computer*' in another country, it is necessary to examine underlying offence elements in the respective criminal laws. Methodologically defensible comparisons of police 'cybercrime' statistics are thus extremely challenging.

Information gathering for the Study included a request to countries to provide the number of police recorded offences corresponding to each of the 14 acts listed in Annex One (Act Descriptions). For each broad act description, respondents were asked to provide available statistics for the years 2008, 2009 and 2010, and to specify whether the data provided corresponded to a

1 United Nations. 2003. *Manual for the Development of a System of Criminal Justice Statistics.*
2 United Nations. Twelfth United Nations Congress on Crime Prevention and Criminal Justice. 2010. *State of Crime and Criminal Justice Worldwide: Report of the Secretary-General.* A/CONF.213/3. 1 February 2010.
3 UNODC calculation from Study cybercrime questionnaire. Q30; and Symantec. 2012. *Norton Cybercrime Report 2012.*
4 Symantec. 2011. *Norton Cybercrime Report 2011.*
5 United States Department of Justice. Federal Bureau of Investigation. 2000. *National Incident-Based Reporting System. Volume 1: Data Collection Guidelines.* Available at http://www.fbi.gov/about-us/cjis/ucr/ucr
6 See, for example, United Nations Economic Commission for Europe, Conference of European Statisticians. *Principles and Framework for an International Classification of Crimes for Statistical Purposes.* ECE/CES/BUR/2011/NOV/8/Add.1. 11 October 2011. Annex I summarizes national offence classification systems.
7 Canadian Centre for Justice Statistics. 2002. Cybercrime*: Issues, Data Sources and Feasibility of Collecting Police-Reported Statistics.*
8 Historical statistics may even include, for example, the number of events of 'motor vehicle theft' or 'burglary/breaking and entering' in which a computer was either the tool or object of the offence. *Ibid.*

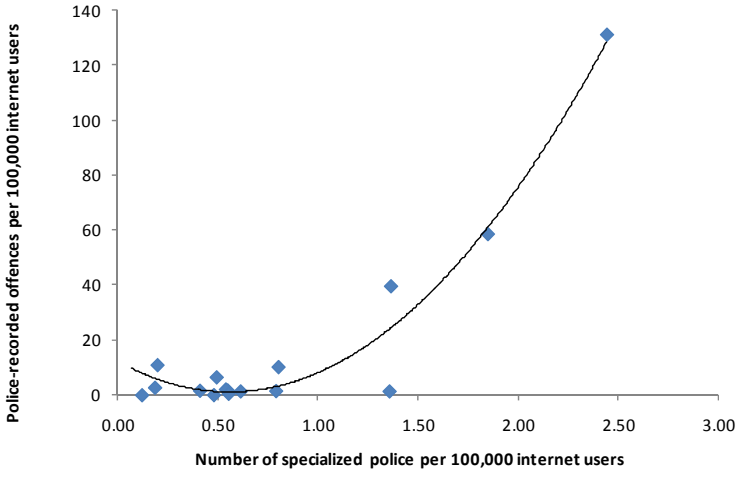
'cyber-specific offence' or to a 'general offence' in law.[9] For example, police-recorded offences for '*illegal access to a computer system*' may be recorded based on a *specific* criminal provision covering this act. Police-recorded offences for '*computer-related fraud or forgery*', on the other hand, may correspond to a sub-set of a *general* fraud offence, in which the involvement of a computer has been identified.

Of those countries that responded to the police statistics questions, across the 14 cybercrime acts (and 3 aggregate categories), under 40 per cent indicated that recorded offence statistics were available. Less than 20 per cent of possible data fields – across all cybercrime acts and years – were completed.[10] This may indicate that many countries experience substantial challenges in collection of police-recorded statistics on cybercrime acts. When asked for the reasons why statistics were not available, a number of countries referred to challenges of disaggregation or aggregation – either that the requested acts were not distinguishable from recorded events, or that existing data could not easily be compiled according to the categories used by the questionnaire.[11] This demonstrates the difficulties in the identification of a common classification of cybercrimes that could be used for statistical purposes. Many countries linked challenges in police statistics with legal frameworks, noting that the absence of a specific legal provision meant that no corresponding police statistical category existed. In cases where a specific provision did not exist, some countries provided estimates. One country for example, provided the *total* number of police-recorded fraud or forgery offences, together with an estimate of the percentage that were committed with the use of a computer system.[12]

For instance, one country said that '*limited resources and the complex nature of 'cybercrime' make it very difficult to gather and analyse statistical information in ways which would provide governments, the private sector, and technology users with a full and accurate picture of the problem. 'Cybercrime' elements are often incidental to other criminal offences, many occurrences are never noticed by victims, or if they are noticed, are often not reported at all (or, if they are reported, only to service providers or credit card companies and not public authorities). An added problem in this area is the fact that many offences are of transnational or uncertain origin, and many offences involve mass-targeting of victims, which can give different statistical pictures depending on what is counted: the single act of sending a fraudulent e-mail to millions of addresses could be counted as one or several million attempts, for example, and might generate thousands of completed offences if the criminal scheme was successful.*'[13]

Examination of police statistics provided shows a number of patterns. Firstly, there are strong indications that – as the comparison with population-based victim survey data suggests – police-recorded cybercrime is not a good indicator for underlying levels of cybercrime. The

Relationship between specialized police and recorded offences (computer-related fraud or forgery)



Source: Study cybercrime questionnaire. Q61 and Q115. (n=44)

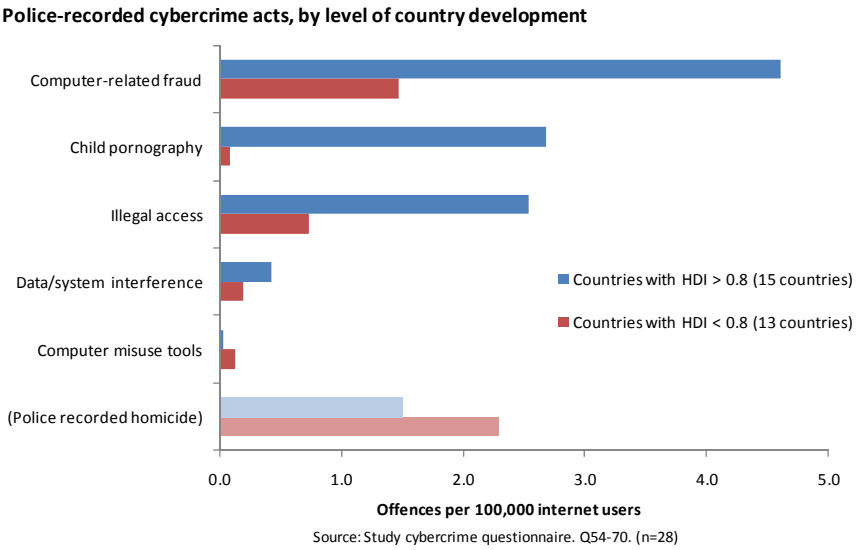
9 Study cybercrime questionnaire. Q54-71.
10 *Ibid.*
11 Study cybercrime questionnaire. Q75.
12 Study cybercrime questionnaire. Q61.
13 Study cybercrime questionnaire. Q76.

rate of police-recorded specific cybercrime offences may be associated both with the level of development of a country and available specialized police capacity.

The number of countries that provided data is comparatively small. However, for this limited group of countries, those with larger numbers of police specialized in cybercrime record a higher number of cybercrime offences – at least for computer-related fraud or forgery.[14] The comparison is shown using the number of specialized police and the number of recorded offences per 100,000 internet users in each country, in order to provide a fair denominator for comparison.[15]

This pattern is probably explained by the fact that only a small percentage of cybercrime acts come to the attention of the police in the first place, and this percentage can likely be increased with the use of additional resources and investigative capacity.[16]

A second pattern relates to police statistics and country development. Four types of police-recorded cybercrime acts – computer-related fraud or forgery, child pornography offences, illegal access to a computer system, and illegal data interference or system interference – are consistently higher per 100,000 internet users in a group of countries with very high levels of human development, than for a group of countries with lower human development. The figure shows the average number of police-recorded offences per 100,000 internet users for 15 countries with HDI greater than 0.8, compared with 13 countries with HDI lower than 0.8.[17] It is possible that absolute levels for at least some of these crimes are indeed higher in more developed countries. Population-based survey results for computer-related consumer fraud, for instance, support a slightly higher victimization level in more highly developed countries.[18] Nonetheless, surveys suggest a reverse picture for other cybercrime acts experienced by individuals – with typically higher levels of victimization in lesser developed countries.[19] The police resource picture, combined with the fact that the comparator of police-recorded homicide[20] is greater in the group of lesser developed countries, may suggest that greater police cybercrime investigative



[14] Study cybercrime questionnaire. Q115 and Q61.

[15] Number of internet users sourced from World Telecommunication/ICT Indicators 2012. The number of internet users is used as the base, rather than the total population, as persons not online are, in principle, not vulnerable to victimization for the vast majority of cybercrime acts – notwithstanding examples such as illegal acquisition of computer data from a standalone computer.

[16] See, for example, Harrendorf, S., Smit, P. 2010. Attributes of criminal justice systems – resources, performance and punitivity. *In*: European Institute for Crime Prevention and Control Affiliated with the United Nations (HEUNI). *International Statistics on Crime and Justice*. Helsinki.

[17] Study cybercrime questionnaire. Q55, Q57, Q58, Q61, and Q68.

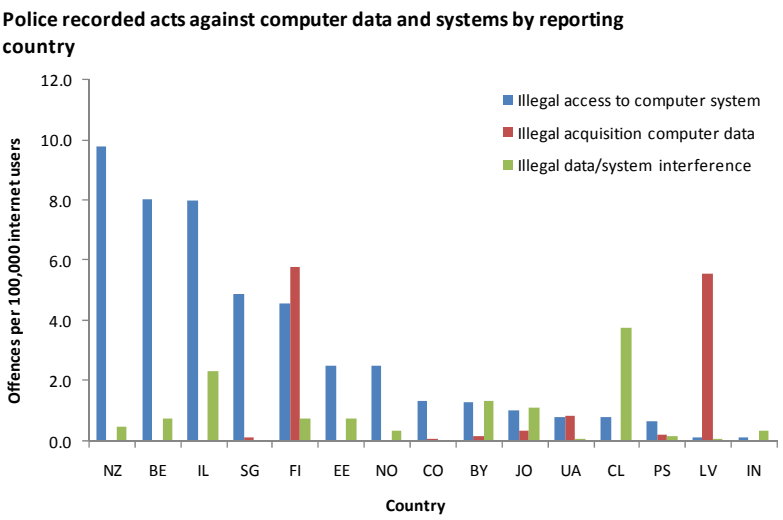
[18] See, for instance, Van Dijk, K.J.M., Van Kesteren, J.N., and Smit, P. 2008. *Criminal Victimization in International Perspective. Key findings from the 2004-2005 ICVS and EU ICS*. The Hague: Boom Legal Publishers.

[19] For instance, with relation to child pornography, see UNODC. 2010. *The Globalization of Crime: A Transnational Organized Crime Threat Assessment*, chapter 10.

[20] Rates for police-recorded homicide are presented per 100,000 population, rather than per 100,000 internet users.

capacity in developed countries is responsible, in part, for driving the large differences between the two groups of countries examined.

A second pattern that complicates interpretation of police-recorded cybercrime statistics concerns differences in the comparative use of offences by law enforcement agencies. The acts of illegal access to a computer system, illegal acquisition of computer data, and illegal data interference or system interference typically represent distinct conduct in law. In practice, however, they may often be combined in a single course of conduct – such as the 'hacking' of a computer system, the copying of computer data from the system, and the corruption of data on the system. One, two, or three separate offences may be recorded by the police, depending upon the availability of evidence, the characterization of the conduct, policy priorities, and offence counting rules.[21] Examination of police-recorded statistics for three offences in the '*acts against the confidentiality, integrity and availability of computer systems or data*' category show significant variation by country. No clear relationship exists between the three offences. It is not the case, for instance, that all categories show roughly equivalent levels in each country. Rather, in some countries, one category is higher than the other two categories. In other countries, two categories are higher. A number of countries did not have statistics available for all three categories. While it cannot be proven that the differences do not reflect real underlying offence characteristics, such diversity is more likely to be significantly affected by investigatory and recording effects.



Source: Study cybercrime questionnaire. Q54-70.

Improvement of police cybercrime statistics

- Installation of a flag in the recording system to identify a cyber-element to crimes
- Establishment of a single centralized reporting body for law enforcement and criminal justice statistics
- Development of standardized counting rules – in particular for acts that target multiple victims (such as 'phishing')
- Further development of crime classification systems to reflect cybercrime

When asked about the *sufficiency* of the current system of police statistics for recording cybercrime acts, two-thirds of responding countries thought that their national system was not sufficient.[22] Respondents noted that police statistics recording systems could be improved in a number of ways. These are detailed in the Box on this page.[23]

Despite such limitations, countries indicated that police-recorded cybercrime statistics were

21 Application of the principle offence rule, for example, may result in the recording of only the most serious offence in a course of conduct. Half of responding countries indicated that a principle offence rule was applied for counting of police-recorded offences. Study cybercrime questionnaire. Q73.

22 Study cybercrime questionnaire. Q76.

23 *Ibid.*

important for policy development in combating cybercrime. One country, for example, stated that '*every four years, police statistics, combined with information on the impact, threat and vulnerability of different kind of crime, including cybercrime, are analysed in a National Police Security Image. This image is used to set the priorities in the National Security Plan for police and justice.*'[24]

Many countries highlighted that police statistics should not be used in isolation. Rather, they are best combined with other data sources. Countries noted that this was especially the case for cybercrime, as the long process of generating police-recorded statistics may not match the pace of technological change or cybercrime trend developments. As such, information from expert assessment of actual and anticipated technological changes, as well as experience with actual offences and case law development, should be integrated with statistical trends. Other countries mentioned that police-recorded cybercrime statistics were important for informing legislative reform processes, and for raising public awareness about the nature and extent of cybercrime.[25]

Population-based and business surveys

Crime victimization surveys are routinely promoted as one of the most effective ways of collecting crime statistics. They remove, in principle, the uncertainty of the 'dark figure' of crime that is not reported to the police, by gathering information directly from the population of potential victims.[26] At the same time, crime victimization surveys have their own methodological challenges, including the need to accurately identify the target population, to design an appropriate survey instrument and sample frame, and to adequately address survey non-response.[27] Nonetheless, where standard methodology and question wording is adopted, crime victimization surveys can offer a reasonable degree of cross-national comparability.[28]

International and national crime victimization surveys have not, to date, systematically incorporated standardized questions relating to cybercrime. Some national population-based surveys cover *'negative experiences when using the internet,'*[29] *'malware incidents,'*[30] or *'computer-related threats of harm or assault'* or *'internet fraud.'*[31] Other national surveys cover related crimes that may or may not involve computer systems or data, including *'identity theft'*[32] and *'cloning of bank cards.'*[33] Regional surveys have also included questions on *'receipt of emails fraudulently asking for money.' 'online fraud where goods purchased were not delivered, counterfeit or not as advised'* and *'accidently encountering material which promotes racial hatred or religious extremism.'*[34] International surveys, such as the ICVS,[35] include only one question directly related to cybercrime – concerning fraud encountered during internet shopping.[36] Population-based surveys conducted by the private sector have asked about *'responding to a fake email or website which capture personal details'*, '*online bullying, stalking, hate crime or harassment,' 'hacking into an email account or social networking profile,' 'online credit card fraud,'*[37] and *'data theft committed over the internet.'*[38]

---

24 Study cybercrime questionnaire. Q77.
25 *Ibid.*
26 For a general review on crime victimization survey methodology, see UNODC/UNECE. 2010. Manual on Victimization Surveys.
27 *Ibid.*
28 See, for example, Van Dijk, K.J.M., Van Kesteren, J.N., and Smit, P. 2008. *Criminal Victimization in International Perspective. Key findings from the 2004-2005 ICVS and EU ICS*. The Hague: Boom Legal Publishers.
29 United Kingdom Home Office. 2012. *Hate crime, cyber security and the experience of crime among children: Findings from the 2010/11 British Crime Survey: Supplementary Volume 3 to Crime in England and Wales 2010/11*.
30 AusCert. 2008. *Home Users Computer Security Survey 2008*.
31 Hong Kong UNICVS. 2010. *Final Report of the 2006 Hong Kong UNICVS*.
32 United States Department of Justice, Bureau of Justice Statistics. 2008. *Identity Theft Supplement to the National Crime Victimization Survey 2008*.
33 INEGI. 2012. *Encuesta Nacional de Victimizacíon y Percepcíon sobre Seguridad Pública 2012 (ENVIPE), Cuestionario Principal.*
34 European Commission. 2012. *Special Eurobarometer 390: Cybersecurity*.
35 For details on the International Crime Victims Survey, see http://www.crimevictimsurvey.eu and http://rechten.uvt.nl/icvs
36 The ICVS 2010 questionnaire included a follow-up questionnaire for respondents who indicated that they had been a victim of consumer fraud. The question asked 'How did this fraud take place? Was it to do with [shopping on the internet?]'
37 Symantec. 2012. *Norton Cybercrime Report 2012*.

Private sector organizations further conduct surveys of cybercrime victimization experienced by businesses.[39] While some of these surveys may make use of a statistical sample frame, the majority are surveys of customers, or selected 'key informants.' A few national government surveys have also covered victimization of businesses.[40] In addition, the Eurostat Community survey on ICT usage in enterprises has recently covered issues of cybercrime and cybersecurity in a dedicated module.[41] Questions asked in business surveys often use the language of 'security incident' to cover a broad range of cybercrime acts, including illegal access by outsider system penetration or hacking, system/data interference in the form of a malware infection or DDoS attack, computer-related fraud perpetrated by 'insiders,' or illegal acquisition of computer data in the form a 'data breach.'

Significant diversity exists in the use of terminology, in the way in which questions are asked, and the frequency of inclusion of cybercrime-related questions in victimization surveys. It is not uncommon for cybercrime questions to be included as special 'modules' to core periodic victimization surveys – making it difficult to construct time series data. While a few surveys do include developing countries,[42] the focus is predominantly on developed countries, leaving an urgent need for survey data from a large part of the world. During information gathering for this Study, very few countries were able to supply information on population-based surveys or business surveys relevant to cybercrime.[43] Where survey data are available, they have been subject to a number of criticisms – including the difficulties in obtaining a sample that is representative not only of the population at risk, but also of the population of losses due to cybercrime.[44]

Further development of survey methodology and question structure will be critical to future efforts in measuring the nature and extent of cybercrime. While cybercrime is – in some respects – a difficult crime to measure due to definitional and lack-of-awareness factors, precedents do exist for the adaptation of victimization survey methodologies to other hard-to-measure crimes, such as violence against women.[45] In addition, recent developments in the ICVS have focused on testing internet-based survey methodologies[46] – an important step where the population of interest is 'internet-users.' A recent 'road-map' for improving crime statistics at the national and international level further highlights the importance of developing and testing statistical surveys for the collection of data on specific forms of cybercrime.[47] Within this Study, statistical data from one of the few cross-nationally comparable population-based surveys is used in the section on 'The global cybercrime picture.'

Victim reporting initiatives

Victims of cybercrime may often prefer to report the act to a designated cybercrime reporting centre, such as a website or hotline, rather than through traditional police channels

---

38 McAfee/National Cybersecurity Alliance. 2012. *Online Safety Survey*.

39 See, for example, Computer Security Institute. 2011. *CSI Computer Crime and Security Survey 2010/2011*; PricewaterhouseCoopers. 2012. *Global State of Information Security Survey*; Ponemon/Check Point Software Technologies. 2012. *The Impact of Cybercrime on Business*; and Ponemon/HP Enterprise Security. 2012. *Cost of Cybercrime Study 2012*.

40 See, for example, United States Department of Justice, Bureau of Justice Statistics. 2006. *National Computer Security Survey*; and Australian Institute of Criminology. 2009. *The Australian Business Assessment of Computer User Security: A National Survey*.

41 Eurostat. 2011. *Community survey on ICT usage and e-commerce in enterprises*. Available at http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/ICT_security_in_enterprises

42 See, for example, Symantec. 2012. *Norton Cybercrime Report 2012* (includes South Africa), and PricewaterhouseCoopers. 2011. *Cybercrime: Protecting against the Growing Threat. Global Economic Crime Survey* (covers 78 countries, including 13 in Africa).

43 Study cybercrime questionnaire. Q10.

44 Florêncio, D., and Herley, C. 2011. *Sex, Lies and Cybercrime Surveys*. Available at: http://research.microsoft.com/pubs/149886/sexliesandcybercrimesurveys.pdf

45 See Johnson, H., and Nevala. S. 2010. *International Violence Against Women Survey (IVAWS)*.

46 See http://crimevictimsurvey.eu

47 United Nations Statistical Commission. 2012. *Report of the National Institute of Statistics and Geography of Mexico and UNODC on Crime Statistics: A Road-map to Improve Crime Statistics at National and International Level*. E/CN.3/2013/11 of 19 December 2012.

(although there are usually close links between reporting centres and law enforcement authorities). Such reporting initiatives exist in a number of countries, including in Southern Asia,[48] Central America,[49] Western Europe,[50] and North America.[51] Victim self-reporting sites are also increasingly found in a number of developing countries, such as in Western Africa.[52] In the same way as police statistics, data derived from cybercrime reporting centres suffer from a significant 'dark figure' of unreported events. They are therefore usually not appropriate for use in cross-national comparisons of cybercrime levels. Even trends in complaints may well be driven as much by levels of victim awareness, as by underlying events.[53]

Nonetheless, statistics derived from victim reporting mechanisms can provide insights into the distribution of cybercrime acts within a particular country. Statistics may show, for example, characteristics such as major computer-related fraud types reported, the distribution of the age and sex of reporting victims, or the nature of illegal content reported.[54] As in the case of police-recorded statistics, comparability of data from victim reporting initiatives may be strengthened by the development of standardized classifications for cybercrime acts.

Technology-based cybersecurity information

Cybercrime acts are perhaps unique amongst crime in general, in that widespread technology-based prevention measures exist – including anti-virus and network security products and firewalls.[55] The role of such products is usually based on scanning, identifying and filtering for certain electronic 'signatures.' These may be content-based, or traffic-based, such as communications to or from 'blacklisted' IP addresses.[56] Many products also include heuristic detection that examines the behaviour of suspect files and connections against pre-determined conditions. The activity logs created by technology-based security products thus capture a sub-set of computer content and traffic events that may – in some circumstances – correspond to components of a cybercrime act. Attempted or completed acts of illegal access to a computer system, or illegal interference with a computer system or computer data may, for example, be detected by and generate a response from such products. A loose analogy is of the household burglar alarm that detects events at household doors and windows. The fact that an alarm is triggered does not necessarily mean that a crime has been committed. A certain proportion of crimes may, nonetheless, trigger the alarm.

An advantage of technology-based cybersecurity products is that very large numbers of 'burglar alarms' may report logged events to a central location – allowing the production of aggregate cybersecurity statistics. Many private sector cybersecurity providers produce reports based on these statistics.[57] Providers often use, however, markedly different definitions; counting methods;

---

48 See http://www.cybercellindia.com/#

49 See http://fiscalia.chihuahua.gob.mx/intro/?page_id=3029

50 See https://www.meldpuntcybercrime.nl/english_information.html; http://www.cybercrime.admin.ch/content/kobik/en/home/meldeformular.html; and http://www.actionfraud.police.uk/home

51 See http://www.ic3.gov/default.aspx

52 See http://cybercrime.interieur.gouv.ci/?q=node/4

53 Annual reports to the United States IC3 reporting centre, for example, increased consistently from the year 2000 to 2009 until levelling off in 2010 and 2011. See Internet Crime Complaint Centre. 2011. *Internet Crime Report 2011*. In contrast, the number of reports received by the Swiss reporting centre decreased from 2007 to 2011. See Service de Coordination de la Lutte Contre la Criminalité sur Internet (SCOCI) 2011. *Rapport Annuel 2011*. Awareness of reporting mechanisms may increase over time or decrease over time, depending on factors such as the degree and consistency of publicity accompanying the mechanism.

54 *Ibid.*

55 See OECD. 2002. *Recommendation of the Council Concerning Guidelines for the Security of Information Systems and Networks Towards a Culture of Security*. 25 July 2002 - C(2002)131/FINAL.

56 Callanan, C., Gercke, M., De Marco, E., and Dries-Ziekenheiner, H. 2009. *Study on Internet blocking, balancing cybercrime responses in democratic societies*. Aconite Internet Solutions, October 2009.

57 See for example AVG. 2011. *Community Powered Threat Report 2012*; Cisco 2011. *Cisco Threat Report 2011*; IBM. 2011. *IBM Trend and Risk Report 2011*; McAfee 2012. *McAfee Threats Report. First Quarter 2012*; Microsoft. 2011. *Microsoft Security Intelligence Report. Volume 12*; PandaLabs. 2012. *PandaLabs Quarterly Report. April-June 2012*; Sophos. 2012. *Security Threat Report 2012*; Symantec. 2011. *Internet*

time series; geographical coverage; and data presentations.[58] As a result, comparison of statistics across 'threat reports' produced by the private sector is extremely challenging. In some cases, such data are presented as 'cybercrime' statistics.[59] It may be more appropriate, however, to view technology-based cybersecurity information as indicative of cybersecurity phenomena that may, or may not, constitute cybercrime acts.

Nonetheless, information on electronic 'threats' from cybersecurity products can be used, with some caution, to assist in understanding broad patterns in the first cybercrime category: acts against the confidentiality, integrity and availability of computer data or systems. Such information can have, in particular, a high degree of cross-national comparability, as the same product – using the same data collection and processing system – is likely to be installed in multiple computer systems across different countries. This Study makes use of technology-based cybersecurity information to characterize one particular tool, the botnet, often used in cybercrime acts.

A majority of countries reported the inadequacy of police statistics for recording cybercrime acts. While a slight majority of European nations reported that police statistics were able to sufficiently capture cybercrime acts, in all other regions, a substantial majority of countries reported that police statistics were not sufficient for recording those cases.

Security Threat Report. 2011 Trends, Volume 17; Total Defense. 2011. *Threat Report: End of Year 2011*; and Trend Micro. 2011. *TrendLabs Annual Security Roundup*.

58 *Ibid*. See also PricewaterhouseCoopers. 2012. E*ye of the storm. Key findings from the 2012 Global State of Information Security Survey; World Economic Forum*. 2012. Global Risks 2012, 7th ed.

59 See, among others, Symantec. 2011. *Internet Security Threat Report. 2011 Trends, Volume 17*.

ANNEX THREE: PROVISIONS OF INTERNATIONAL AND REGIONAL INSTRUMENTS

Definitions	African Union[1]	COMESA[2]	The Commonwealth[3]	Commonwealth of Independent States[4]	Council of Europe[5] (Budapest Convention and OP)	Council of Europe[6] (Lanzarote Convention)	ECOWAS[7]	European Union[8] (Framework Decision 2005/222/JHA)	European Union[9] (Directive Proposal 2010/0273)	European Union[10] (Framework Decision 2001/413/JHA)	European Union[11] (Directive 2011/92/EU)	ITU/CARICOM/CTU[12] (Model Legislative Texts)	League of Arab States[13] (Convention)	League of Arab States[14] (Model Law)	Shanghai Cooperation Organization[15]	United Nations[16] (CRC OP)
Computer/information system	Art. III-1(6)	Arts. 1(b) 1(e) 1(n)	Art. 3		Art. 1(a)		Art. 1	Art. 1(a)	Art. 2(a)			Arts. 3(5) 2(6)* 2(17)*	Arts. 2(1) 2(5)	Art. 1		
Computer/information network		Art. 1(s)											Art. 2(6)	Art 1		
Device/storage media			Art. 3									Arts. 3(7) 3(9)				
Critical infrastructure		Art. 1(g)										Art. 3(8)			Annx 1	
Computer data/ information (including computer program)	Art. III-1(2)	Arts. 1(c) 1(d) 1(j)	Art. 3	Art. 1(b)	Art. 1(b)		Art. 1	Art. 1(b)	Art. 1(b)			Arts. 3(6) 2(9)*	Art. 2(3) 2(4)	Art. 1		
Electronic record		Art. 1(j)	Art, 2*									Art. 2(15)*				
Subscriber/traffic/ content data/ information		Arts. 1(f) 1(u) 1(v)	Art. 3		Arts. 1(d) 18							Arts. 3(18) 2(7)* 2(27)* 2(28)*	Art. 2(9)			
Electronic communication/mail	Art. III-1(1)	Art. 1(m)					Art. 1					Art. 2(14)*				
Malware/malicious software		Art. 1(r)		Art. 1(c)												
(Internet) service provider		Art.1 1(t)	Art. 3		Art.1 (c)							Arts. 3(1) 3(2) 3(11) 3(17)	Art. 2(2)			
Child/minor	Art. III-1(4)		Art. 10(3)		Art. 9(3)	Art. 3	Art. 1				Art. 2(a)	Art. 3(3)				Art. 2(c)

Definitions	African Union[1]	COMESA[2]	The Commonwealth[3]	Commonwealth of Independent States[4]	Council of Europe[5] (Budapest Convention and OP)	Council of Europe[6] (Lanzarote Convention)	ECOWAS[7]	European Union[8] (Framework Decision 2005/222/JHA)	European Union[9] (Directive Proposal 2010/0273)	European Union[10] (Framework Decision 2001/413/JHA)	European Union[11] (Directive 2011/92/EU)	ITU/CARICOM/CTU[12] (Model Legislative Texts)	League of Arab States[13] (Convention)	League of Arab States[14] (Model Law)	Shanghai Cooperation Organization[15]	United Nations[16] (CRC OP)
Cybercrime/computer crime				Art.1 (a)											Annx 1	

Criminalization	African Union[1]	COMESA[2]	The Commonwealth[2]	Commonwealth of Independent States[4]	Council of Europe[5] (Budapest Convention)	Council of Europe[6] (Lanzarote Convention)	ECOWAS[7]	European Union[8] (Framework Decision 2005/222/JHA)	European Union[9] (Directive Proposal 2010/0273)	European Union[10] (Framework Decision 2001/413/JHA)	European Union[11,17] (Directive 2011/92/EU and 2002/58/EC)	ITU/CARICOM/CTU[12] (Model Legislative Texts)	League of Arab States[13] (Convention)	League of Arab States[14] (Model Law)	Shanghai Cooperation Organization[15]	United Nations[16] (CRC OP)
Illegal access to a computer system	Arts. III(15) III(16)	Arts. 18 19	Arts. 5 7		Art. 2		Arts. 2 3	Art. 2(1)	Art. 3			Arts. 4 5	Art. 6	Arts. 3, 5 15 22		
Illegal access, interception or acquisition of computer data	Art. III(23)	Arts. 19 21	Arts. 5 8	Art. 3(1) (a)	Arts. 2 3		Art. 6		Art. 6			Arts. 6 8	Arts. 6 7 18	Arts. 3 8		
Illegal interference with computer data	Arts. III(19) III(20) III(24)	Arts. 20 22(a)	Art. 6	Art. 3(1) (c)	Art. 4		Arts. 5 7	Art. 4	Art. 5	Art. 3		Art. 7	Art. 8	Art. 6		
Illegal interference with a computer system	Arts. III(18) III(19)	Art. 22(a)	Art. 7	Art. 3(1) (c)	Art. 5		Art. 4	Art. 3	Art. 4	Art. 3		Art. 9	Art. 6	Art. 7		
Computer misuse tools	Art. III(22)	Art. 22(b) 22(c)	Art. 9	Art. 3(1) (b)	Art. 6		Art. 12	Art. 5	Art. 7	Art. 4		Art. 10	Art. 9			
Breach of privacy or data protection measures	Arts. III(27) III(54)			Art. 3			Art. 11				Art. 15 (a) (1)[1]					
Computer-related forgery	Arts. III(24) III(25)	Art. 23			Art. 7		Art. 8			Arts. 2 4		Art. 11	Arts. 10 18	Art. 4		

1 Directive 2002/58/EC (not a strict criminalization requirement).

Criminalization	African Union [1]	COMESA [2]	The Commonwealth [3]	Commonwealth of Independent States [4]	Council of Europe [5] (Budapest Convention)	Council of Europe [6] (Lanzarote Convention)	ECOWAS [7]	European Union [8] (Framework Decision 2005/222/JHA)	European Union [9] (Directive Proposal 2010/0273)	European Union [10] (Framework Decision 2001/413/JHA)	European Union [11,17] (Directive 2011/92/EU and 2002/58/EC)	ITU/CARICOM/CTU [12] (Model Legislative Texts)	League of Arab States [13] (Convention)	League of Arab States [14] (Model Law)	Shanghai Cooperation Organization [15]	United Nations [16] (CRC OP)
Computer-related fraud	Arts. III(25) III(26) III(41)	Art. 24(a) 24(b)			Art. 8		Arts. 9 10 23			Arts. 2 4		Art. 12	Art. 11	Arts. 10 11 12		
Electronic payment tools offences										Art. 2			Art. 18	Art. 11		
Identity-related crime												Art. 14				
Computer-related copyright and trademark offences				Art. 3(1) (d)	Art. 10								Art. 17	Art. 14		
Spam		Art. 19(g)									Art. 13(3)[2]	Art. 15				
Computer-related harassment, extortion, or acts causing personal harm	Arts. III(40) III(41)	Art. 25										Art. 18		Art. 9		
Computer-related acts involving racism or xenophobia	Art. III(34) III(35) III(36)				Art. 3,4,5 (OP)		Arts. 18,19 20									
Computer-related denial or justification of genocide or crimes against humanity	Art. III(37)				Art. 6 (OP)		Art. 21									
Computer-related production, distribution, or possession of child pornography	Arts. III(29) III(30) III(31) III(32)		Art. 10		Art. 9	Art. 20	Art. 14-17				Art. 5	Art. 13	Art. 12			Art. 3
Computer-related solicitation or 'grooming' of children						Art. 23					Art. 6					
Computer-related acts in support of terrorism	Art. III(40)	Arts. 18 19 20 22(a)											Art. 15	Art. 21		

[2] Directive 2002/58/EC (not a strict criminalization requirement).

Criminalization	African Union [1]	COMESA [2]	The Commonwealth [2]	Commonwealth of Independent States [4]	Council of Europe [5] (Budapest Convention)	Council of Europe [6] (Lanzarote Convention)	ECOWAS [7]	European Union [8] (Framework Decision 2005/222/JHA)	European Union [9] (Directive Proposal 2010/0273)	European Union [10] (Framework Decision 2001/413/JHA)	European Union [11,17] (Directive 2011/92/EU and 2002/58/EC)	ITU/CARICOM/CTU [12] (Model Legislative Texts)	League of Arab States [13] (Convention)	League of Arab States [14] (Model Law)	Shanghai Cooperation Organization [15]	United Nations [16] (CRC OP)
Computer-related offences involving money laundering													Art. 15	Art. 19		
Computer-related offences involving illicit trafficking													Art. 16	Arts. 17 18		
Computer-related offences against public order, morality or security							Arts. 14 15 16 17						Arts. 12 13 14 15	Arts. 13 16 20		
Law enforcement investigation-related offences	Art. III(54)		Arts. 13 21		Arts. 16(3) 20(3) 21(3)							Arts. 16 17	Arts. 23(3) 28(3) 29(3)			
Aggravating circumstances for conventional crime committed by means of a computer system	Art. III(40)						Art. 22						Art. 21			
Attempt and aiding or abetting		Art. 26			Arts. 11 7(OP)	Art. 24			Art. 8							
Corporate liability		Art. 27			Art. 12	Art. 26										

Procedural powers	African Union [1]	COMESA [2]	The Commonwealth [2]	Commonwealth of Independent States [4]	Council of Europe [5] (Budapest Convention)	Council of Europe [6] (Lanzarote Convention)	ECOWAS [7]	European Union [8] (Framework Decision 2005/222/JHA)	European Union [9] (Directive Proposal 2010/0273)	European Union [18] (Directive 2006/24/EC)	European Union [11] (Directive 2011/92/EU)	ITU/CARICOM/CTU [12] (Model Legislative Texts)	League of Arab States [13] (Convention)	League of Arab States [14] (Model Law)	Shanghai Cooperation Organization [15]	United Nations [16] (CRC OP)
Search for computer hardware or data	Art. III(50)	Arts. 37(a) 37(b)	Art. 12		Arts. 19(1) 19(2)		Art. 33					Art. 20	Art. 26			
Seizure of computer hardware or data	Art. III(51)	Art. 37(c)	Arts. 12 14		Art. 19(3)		Art. 33					Art. 20	Art. 27(1)			

Order for stored computer data		Art. 36(a)	Art. 15		Art. 18(1)(a)							Art. 22(a)	Art. 25(1)			
Order for subscriber information		Art. 36(b)			Art. 18(1)(b)							Art. 22(b)	Art. 25(2)			
Order for stored traffic data		Art. 34(a)(ii)	Art. 16		Art. 17(1)(b)							Art. 24	Art. 24			
Real-time collection of traffic data		Art. 38	Art. 19		Art. 20							Art. 25	Art. 28			
Real-time collection of content data	Art. III(55)	Art. 39	Art. 18		Art. 21							Art. 26	Art. 29			
Expedited preservation of computer data	Art. III(53)	Arts. 33 34(a)(i) 35	Art. 17		Arts. 16 17(1)(a)		Art. 33					Art. 23	Art. 23(2)			
Use of (remote) forensic tools						Art. 30(5)					Art. 15	Art. 27				
Trans-border access to computer data		Art. 49(b)			Art. 32(b)								Art. 40(2)			
Provision of assistance		Art. 37(d)	Art. 13		Art. 19(4)							Art. 21	Art. 27(2)			
Retention of computer data		Arts. 29 30 31								Arts. 3 6						

Electronic evidence	**African Union** [1]	**COMESA** [2]	**The Commonwealth** [3]	**Commonwealth of Independent States** [4]	**Council of Europe** [5] (Budapest Convention)	**Council of Europe** [6] (Lanzarote Convention)	**ECOWAS** [7]	**European Union** [8] (Framework Decision 2005/222/JHA)	**European Union** [9] (Directive Proposal 2010/0273)	**European Union** [10] (Framework Decision 2001/413/JHA)	**European Union** [11] (Directive 2011/92/EU)	**ITU/CARICOM/CTU** [12] (Model Legislative Texts)	**League of Arab States** [13] (Convention)	**League of Arab States** [14] (Model Law)	**Shanghai Cooperation Organization** [15]	**United Nations** [16] (CRC OP)
Admissibility of electronic evidence/records	Art. I(24)	Art. 5(a)	Arts. 20 3* 11*				Art. 34					Arts. 5* 7(1)* 12*				
Admissibility of electronic signature			Art. 12									Art. 14*				
Burden of proving authenticity			Art. 5*									Art. 9*				
Best evidence rule			Art. 6*									Art. 6*				

Print-outs as best evidence												Art. 8*				
Presumption of integrity			Art. 7*									Art. 7(2)*				
Evidence on recording/ preservation standards			Art. 8*									Art. 10*				
Electronic evidence/records from other countries and foreign documents												Art. 16* 17*				

Jurisdiction	**African Union** [1]	**COMESA** [2]	**The Commonwealth** [3]	**Commonwealth of Independent States** [4]	**Council of Europe** [5] (Budapest Convention)	**Council of Europe** [6] (Lanzarote Convention)	**ECOWAS** [7]	**European Union** [8] (Framework Decision 2005/222/JHA)	**European Union** [9] (Directive Proposal 2010/0273)	**European Union** [10] (Framework Decision 2001/413/JHA)	**European Union** [11] (Directive 2011/92/EU)	**ITU/CARICOM/CTU** [12] (Model Legislative Texts)	**League of Arab States** [13] (Convention)	**League of Arab States** [14] (Model Law)	**Shanghai Cooperation Organization** [15]	**United Nations** [16] (CRC OP)
Territorial principle		Art. 40 (a)(i)	Art. 4(a)		Art. 22 (1)(a)	Art. 25 (1)(a)		Art. 10 (1)(a)	Art. 13 (1)(a)	Art. 9 (1)(a)	Art. 17 (1)(a)	Art. 19(a)	Art. 30 (1)(a)			Art. 4(1)
Using a computer system/data located within the territory		Art. 40 (a)(ii)														
Directed against a computer system/data located within the territory		Art. 40 (a)(iii)						Art. 10 (2)(b)	Art. 13 (2)(b)							
Nationality principle (offender)		Art. 40(c)	Arts. 4(c),(d)		Art. 22 (1)(d)	Art. 25(1) (d)		Art. 10 (1)(b)	Art. 13 (1)(b)	Art. 9 (1)(b)	Art. 17 (1)(b)	Art. 19(c)	Art. 30 (1)(d)			Art. 4 (2)(a)
Nationality principle (victim)						Art. 25(2)					Art. 17 (2)(a)					Art. 4 (2)(b)
Habitual residence principle						Arts.25(1) (e) 25(2) 25(5)			Art. 13 (1)(b)		Arts. 17 (2)(a) (2)(c)					Art. 4 (2)(a)
Legal person – incorporation principle								Art. 10 (1)(c)	Art. 13 (1)(c)	Art. 9 (1)(c)	Art. 17 (2)(b)					
State interests principle													Art. 30 (1)(e)	Art. 26		
Jurisdiction when extradition refused		Arts. 40(d)			Art. 22(3)	Art. 25(7)		Art. 10(3)		Art. 10(1)			Art. 30(2)			Art. 4(3)

Ships and aircraft		Art. 40(b)	Art. 4(b)		Arts. 22 (1)(b) (c)	Arts. 25 (1)(b) (c)						Art. 19(b)	Arts. 30 (1)(b) (c)			Art. 4(1)
Dual criminality			Art. 4(d)		Art. 22 (1)(d)					Art. 9 (1)(b)	Art. 17(4)	Art. 19	Art. 30 (1)(d)			
Concurrent jurisdiction		Art. 40(e)			Art. 22(5)	Art. 25(8)		Art. 10(4)					Art. 30(3)			
Establishment of place of offence		Art. 40(f)									Art. 17(3)					

International cooperation	**African Union** [1]	**COMESA** [2]	**The Commonwealth** [3]	**Commonwealth of Independent States** [4]	**Council of Europe** [5] (Budapest Convention)	**Council of Europe** [6] (Lanzarote Convention)	**ECOWAS** [7]	**European Union** [8] (Framework Decision 2005/222/JHA)	**European Union** [9] (Directive Proposal 2010/0273)	**European Union** [10] (Framework Decision 2001/413/JHA)	**European Union** [11] (Directive 2011/92/EU)	**ITU/CARICOM/CTU** [12] (Model Legislative Texts)	**League of Arab States** [13] (Convention)	**League of Arab States** [14] (Model Law)	**Shanghai Cooperation Organization** [15]	**United Nations** [16] (CRC OP)
General principle of international cooperation	Art. III(14)	Art. 41		Art. 5	Art. 23	Art. 38(1)									Art. 3-5	Art. 10
Extradition for instrument offences		Art. 42(c)			Art. 24	Art. 38(3)				Art. 10			Art. 31			Art. 5
General mutual legal assistance		Arts. 43(a) 45		Art. 6	Arts. 25 27	Art. 38(3)	Art. 35			Art. 11			Arts. 32 34			Art. 6
Mechanism for expedited assistance		Art. 43(b)		Arts. 6(2) 7(1)	Art. 25(3)								Art. 32(3)			
Assistance – preservation of computer data		Art. 46			Art. 29								Art. 37			
Assistance – seizure/access to/collection of/disclosure of computer data		Arts. 47 48 51			Arts. 30 31 34								Arts. 38 39 41 42			
Trans-border access to computer data		Art. 49(b)			Art. 32(b)								Art. 40(2)			
Provision of unsolicited information/exchange of information		Art. 44			Art. 26			Art. 11	Art. 14	Art. 12			Art. 33			
Confidentiality of request		Art. 45(e)		Art. 9	Art. 28								Art. 36		Art. 6	

Dual criminality		Arts, 42(a), 43(d)			Arts. 24(1), 25(5)								Arts. 32(5) 37(3) 37(4)				
Establishment of point of contact or 24/7 network		Art. 52			Art. 35			Art. 11	Art. 14				Art. 43				

Service Provider Liability and Responsibility	**African Union** [1]	**COMESA** [2]	**The Commonwealth** [3]	**Commonwealth of Independent States** [4]	**Council of Europe** [5] (Budapest Convention)	**Council of Europe** [6] (Lanzarote Convention)	**ECOWAS** [7]	**European Union** [8] (Framework Decision 2005/222/JHA)	**European Union** [9] (Directive Proposal 2010/0273)	**European Union** [10] (Directive 2000/31/EC)	**European Union** [11] (Directive 2011/92/EU)	**ITU/CARICOM/CTU** [12] (Model Legislative Texts)	**League of Arab States** [13] (Convention)	**League of Arab States** [14] (Model Law)	**Shanghai Cooperation Organization** [15]	**United Nations** [16] (CRC OP)
Monitoring obligations		Art. 17								Art. 15		Art. 28				
Voluntary supply of information		Art. 17(b)														
Take-down notifications		Art. 16														
Liability of access providers		Art. 12								Art. 12		Art. 29				
Liability of caching providers		Art. 13								Art. 13		Art. 31				
Liability of hosting providers		Art. 14								Art. 14		Art. 30				
Liability of hyperlink providers/search engines		Art. 15										Art 32, 33				

1 African Union, 2012. Draft Convention on the Establishment of a Legal Framework Conductive to Cybersecurity in Africa.
2 Common Market for Eastern and Southern Africa (COMESA), 2011. Cybersecurity Draft Model Bill.
3 The Commonwealth, 2002. (i) Computer and Computer Related Crimes Bill and (ii) Model Law on Electronic Evidence (indicated by *).
4 Commonwealth of Independent States, 2001. Agreement on Cooperation in Combating Offences related to Computer Information.
5 Council of Europe, 2001. Convention on Cybercrime and Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.
6 Council of Europe, 2007. Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse.
7 Economic Community of West African States (ECOWAS), 2009. Draft Directive on Fighting Cybercrime within ECOWAS.
8 European Union, 2005. Council Framework Decision 2005/222/JHA on attacks against information systems.
9 European Union, 2010. Proposal COM(2010) 517 final for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA.
10 European Union, 2001. Council Framework Decision 2001/413/JHA combating fraud and counterfeiting of non-cash means of payment.

11 European Union, 2011. Directive 2011/92/EU of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

12 International Telecommunication Union (ITU)/Caribbean Community (CARICOM)/Caribbean Telecommunications Union (CTU), 2010. (i) Model Legislative Texts on Cybercrime/e-Crimes and (ii) Electronic Evidence (indicated by *).

13 League of Arab States, 2010. Arab Convention on Combating Information Technology Offences.

14 League of Arab States, 2004. Model Arab Law on Combating Offences related to Information Technology Systems.

15 Shanghai Cooperation Organization, 2010. Agreement on Cooperation in the Field of International Information Security.

16 United Nations, 2000. Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.

17 European Union, 2002. Directive 2002/58/EC of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector.

18 European Union, 2006. Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks.

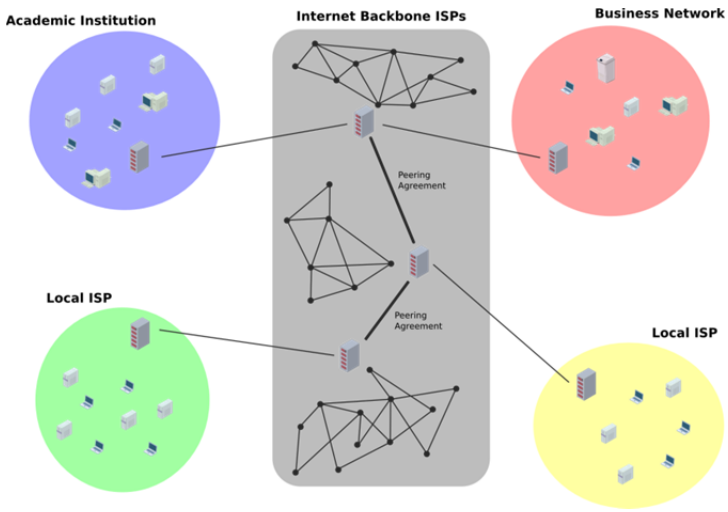
19 European Union, 2000. Directive 2000/31/EC of the European Parliament and of the Council on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

Page left intentionally blank

ANNEX FOUR: THE INTERNET

The internet is a *combination* of networks that communicate between themselves – the word 'internet' is itself simply an abbreviation of the word 'inter-networking.' These networks are ultimately made up of individual computers, ranging from home PCs to supercomputers, which talk to each other through a global infrastructure of physical cables and wireless links.

Routers manage the transfer of data through these networks. They can be small, low-power devices, or powerful machines that handle thousands of individual connections and huge amounts of traffic. Routers join individual computer networks together to make up the internet, transferring information and providing the digital directions that allow computers to connect to each other anywhere in the world.



How the internet works

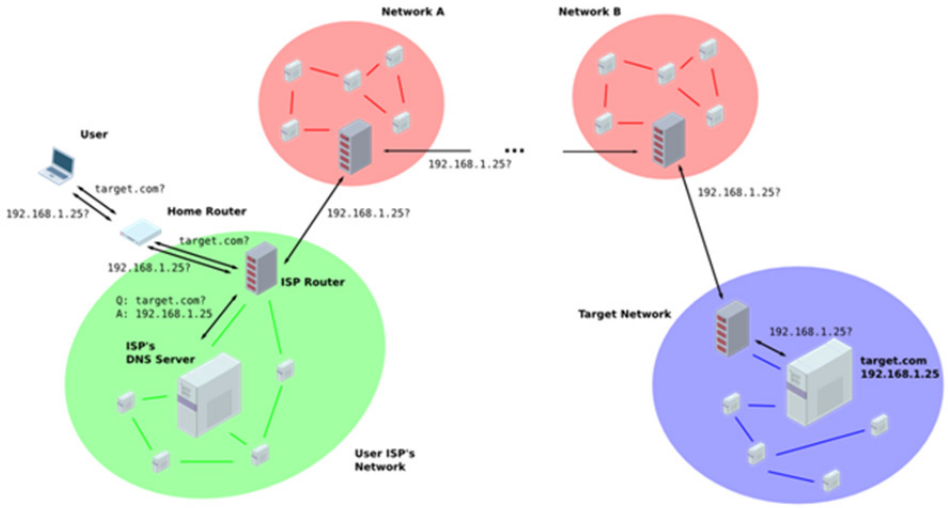
There are many types of internet traffic. The most familiar is related to the *World Wide Web,* which was first developed at the European Organization for Nuclear Research (CERN) at the end of the 1980s. The web was first conceived as a system of documents containing links to other documents – a concept known as 'hypertext' that had been proposed as early as the 1930s.[1]

By clicking on a link in a web browser, a series of operations is initiated which results in the display of a new webpage on a computer. This process is illustrated in the figure below. The first step is to translate the human-readable name of a service, such as www.target.com, to the numerical Internet Protocol (IP) *address* that computers can use to locate other computers on the internet. This is done using a Domain Name System (DNS) server, usually operated by the user's ISP, whose location is usually provided to the user's computer when they first connect. Several alternative DNS servers are available – well known examples are operated by OpenDNS, as well as Google.[2]

Once the IP address of the remote computer is known, information can be sent to it. This can take the form of requests for data, such as a webpage, which is then sent back to the user's web browser. To do this, the information is broken down into a sequence of *packets* – small amounts of data that travel independently over the internet before being remotely reassembled at the remote computer. Each packet contains the IP address of the remote computer, information related to the type of data included in the packet, and the piece of data itself.

1 Ziewitz, M. and Brown, I. 2013. A prehistory of Internet governance. *In* Brown, I.*Research Handbook on Governance of the Internet.* Cheltenham: Edward Elgar.

2 See http://www.opendns.com and https://developers.google.com/speed/public-dns/



Packets do not generally include information on the route to their destination. Instead, much like a postal system, only the destination is given. The routers that the packet encounters will decide the most effective way to reach the destination. By doing so, the internet can respond rapidly and flexibly if part of the network is damaged or overloaded, by choosing alternative paths for data.

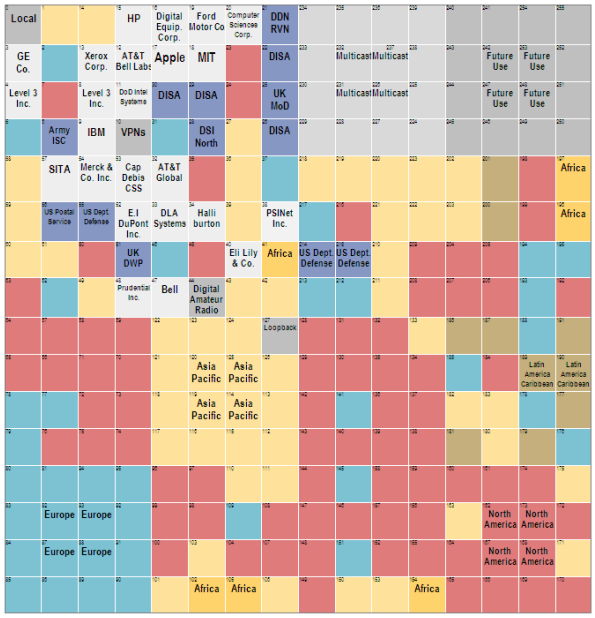
Mechanisms of connectivity

The internet is based around a set of technical standards for transmitting and routing data. The *Internet Protocol* (IP) sets how data is broken down into chunks for transmission, as well as how the source and destination addresses are specified. Version 4 is most commonly used (IPv4), although there is a determined push towards the newer IPv6. In order to build services such as the web, extra protocols are 'layered' on top of the core Internet Protocol. The most common of these is TCP, the *transmission control protocol*, which provides a reliable delivery mechanism and prevents the sending of too much data at one time. Another protocol, UDP, the *user datagram protocol*, provides no guarantees of delivery, but allows highly efficient and flexible transmission for real-time communications such as voice.

Each computer on the internet has a unique address, written in the form of a 'dotted quad' such as 192.168.1.1. Routers use these *IP addresses* to route each packet to its destination. TCP and UDP add 'port numbers' that specify the service the packet is directed to:

Service	**Transport**	**Port Number**
SMTP (Email)	TCP	25
Web (HTTP)	TCP	80
Secure Web (HTTPS)	TCP	443
DNS	UDP	53
SSH (Secure Remote Shell)	TCP	22

The allocation of three sets of unique identifiers for the internet – domain names, IP addresses and autonomous system (AS) numbers, and protocol port and parameter numbers – is overseen by a nonprofit public benefit corporation in the United States of America: ICANN, the *Internet Corporation for Assigned Names and Numbers*.[3] Additionally, ICANN coordinates the operation and evolution of the DNS root name server system, and coordinates policy development related to these technical functions.[4] Functions of allocation and registration of internet resources is delegated to five *regional internet registries* that allocate 'blocks' of IP addresses to organizations such as internet service providers and academic institutions.



There are a limited number of IPv4 addresses available. IPv4 addresses are '32-bit' numbers – numbers that can be expressed in binary using 32 digits – allowing 2^{32}, or roughly 4.3 billion addresses. As the internet has grown beyond all expectations, these numbers are rapidly running out, leaving no space for new devices to be added. In response, a major effort is currently underway to update the internet to a new version of the internet protocol, IP version 6 (IPv6). IPv6 expands the available number of addresses using 128-bit numbers, creating 2^{128} addresses – written in decimal, this number is 39 digits long. It is hoped that this will be enough for the foreseeable future. The figure above shows the current total available and allocated IPv4 address space.[5] Large blocks of available IPv4 addresses are allocated to regional registries. For historical reasons, some top-level blocks, such as 18.x.x.x are also allocated to individual private sector, academic or governmental organizations.

The Domain Name System (DNS)

To be more accessible for human users, addresses on the internet are also written as *domain names* using the Domain Name System. In addition to IP address allocation, ICANN administers the DNS through delegated authority to domain name registries. Such registries consist of databases of all domain names registered in *generic top level demains* (gTLD), such as .com, .net, .int, .mil, .gov, and *country code top level domains* (ccTLD) such as .de (Germany) and .cn (China). Registries are responsible for maintaining the authoritative details of where each domain can be found.

When a new domain is registered, it is typically handled by one of the many dedicated *registrars*. This company checks that the new domain does not already exists, then informs the central registry that a new domain has been requested, along with information about where the authoritative details regarding the domain can be found. This information is then relayed, over the course of

[3] The Articles of Incorporation of the Internet Corporation for Assigned Names and Numbers are available at http://www.icann.org/en/about/governance/articles

[4] Internet Corporation for Assigned Names and Numbers. 2012. *Bylaws for Internet Corporation for Assigned Names and Numbers.*

[5] Internet Assigned Numbers Authority. 2012. *IANA IPv4 Address Space Registry.*

roughly 24 hours, to key DNS servers around the world.

Under each top-level domain are found the names of familiar organizations that have registered the name. The company Google, for example, has registered the name 'google' within the .com top-level domain, to produce the google.com domain. Computers may be given individual names within their domain. The name 'www' is a standard name for the computer that runs a web server, and so is typically seen at the start of a web address such as www.google.com.[6] Similarly mail.google.com points to the computer that offers Google's GMail service. Some TLDs are further subdivided into groups such as .co for businesses or .ac for universities, for example in the UK. This means Google's UK online presence is registered at www.google.co.uk.

ICANN's new gTLD programme will allow the creation of new top-level domains, allowing for names such as .baby or .book to be registered. The complexity and cost of registering new gTLDs are high, but the programme will significantly expand the number of possible alternatives for domain names.

Common Services

One of the most common applications for the early internet was electronic mail, or email, and this remains a major service – an email-address has become as important as a telephone number or physical address for many modern transactions.

Apart from email, the driving force of the internet has been the web, which coincided with the boom in the 1990s of the number of home users going online. Since then, so-called 'Web 2.0' tools have supported the growth of user-generated content. These sites allow users to share their lives and their interests with friends, to upload photos and videos, to create journals or *blogs*, as well as a host of other activities. A third widely-used service is now *voice-over-IP*, or VoIP. This allows phone calls and, increasingly, video and conference calls, to take place cheaply and easily online.

Limited connectivity

Many parts of South and East Africa were first connected to high-speed internet services, via the laying of a submarine cable, as late as 2009. As of 2012, the continent of Africa makes up only 6 per cent of global internet connectivity.

Mobile phone-based internet connections have outnumbered landline-based internet connections since 2008. In much of Africa, despite improvements in the available infrastructure, mobile phones remain by far the most common way of accessing internet-based services. This has led to a range of services aimed at mobile users, from electronic currencies based around mobile phone credits, to search results relayed by SMS text messages.

A final key technology is *peer-to-peer* (P2P) networking, which connects users' computers directly to each other for the purposes of sharing files or data. P2P networking lies in contrast to traditional services where all connections happen through a central *server*. The earliest common P2P networks were Napster and Gnutella, which initially focused on sharing music files. More recently, a system named BitTorrent has allowed for extremely fast and efficient sharing of large files, such as software applications and videos.

BitTorrent works by causing all users to download and upload chunks of data. To distribute a large file, such as a video, BitTorrent splits the file into small chunks. As users download these chunks, they simultaneously make the chunks that they have already downloaded available for others

[6] In reality Google run their website on many different computers. 'www' is actually an *alias* that points to many different computers as required.

to download. The result of this is that as more users download a file, more users share parts of the file, increasing the speed of download for other users. The success of this approach is reflected in the fact that BitTorrent represented between 10 and 15 per cent of total aggregate fixed internet traffic in Europe and North America in the second half of 2012.[7]

Governance

Since its earliest days, a number of institutions have had an influence on the development and functioning of the internet. Some of these are traditional government bodies, others are corporations, still others are volunteer groups.[8]

The principal standards-setting body is the *Internet Engineering Task Force* (IETF). Made up of volunteers from around the world, the IETF develops and adopts new standards for internet technologies, as well as coordinating with other standards bodies. The most well-known of the IETF's outputs are *requests for comments* or RFCs. These describe new internet protocols openly, so that anyone can build compatible technologies.

The *Internet Corporation for Assigned Names and Numbers* (ICANN) manages IP addresses and domain names. ICANN is itself a private non-profit corporation registered in North America. ICANN's organizational structure includes triannual Governmental Advisory Committee (GAC) meetings that provide a forum to receive advice and representation from national governments.

The *International Telecommunication Union* (ITU) sets standards for telegraph and telephone communications, as well as radio spectrum. The International Telecommunication Regulations (ITRs) supplement the International Telecommunication Convention, with a view to establishing general principles which relate to the provision and operation of various aspects of global communications, including traffic flows and quality of service. The ITRs were drafted before the rise of the internet as a dominant international communications platform, and as such do not make specific reference to the internet itself.

Internet routing

When computers send information across the internet, it travels across many networks before reaching its destination. To determine the best route, networks advertise their ability to handle certain routes using a protocol called BGP – the Border Gateway Protocol.

BGP is one of the core protocols on the internet, but has few specific security features in the protocol, and configuration mistakes can have significant consequences. For example, in early 2010, a small ISP in Eastern Asia began to advertise roughly 35,000 routes between networks, rather than its usual 40. The result was that roughly 10 per cent of worldwide networks were reported to have been mistakenly routed for a period of about twenty minutes.

History

The origins of the internet can be traced to a research project conducted by the Advanced Research Projects Agency (ARPA, later DARPA) of the United States Department of Defense, beginning in 1969, that aimed to allow remote access to the then-scarce computing resources hosted by corporate and academic institutions.

The network that arose from this project, known as ARPANET, differed radically from earlier telecommunications networks in employing the newly-developed concept of *packet switching*

7 Sandvine. 2012. *Global Internet Phenomena Report 2H 2012.*

8 Ziewitz, M. and Brown, I. 2013. A prehistory of Internet governance. *In* Brown, I.*Research Handbook on Governance of the Internet.* Cheltenham: Edward Elgar.

rather than the traditional *circuit switching* approach, resulting in much greater robustness and efficiency on the unreliable communication lines available at the time.

ARPANET grew quickly, as did various similar networks in both the United States of America and Europe. As the number of networks grew, ARPA funded research by Vinton Cerf and others to find a way for these networks to communicate with each other. The result of this work was the first specification of the *Internet Transmission Control Protocol* in 1973, which provided a common way for joining together different networks, and contained the first usage of the term 'internet'. The techniques developed for this work remain at the heart of today's internet.

In 1989, Tim Berners-Lee, working at CERN, developed the world-wide web, which allowed documents, or *pages*, to link to other documents stored across a network. Berners-Lee's software was made freely available, and became extremely popular during the early 1990s.

In 1994, early restrictions on commercial activity on the internet were relaxed. This, along with the increasing popularity of the web, caused an explosion of personal and commercial use of the internet during the 1990s. Commercial ISPs connected users to the internet, and to an ever-expanding range of tools and information services. The mid-1990s saw the rise of the first truly large internet-based companies, mainly early search engines, which helped to make sense of the vast array of information now available. Yahoo!, founded in 1994, was an early leader, with Google following in 1998.

Since then, simple and static websites have given way to interactive sites that allow users to create and share content, leading to the rise of social networking. Speed of connection has exploded, allowing videos and music to be streamed to home computers.

Targeted adverts

The dominant business model of the web is advertising. Popular websites such as Google, Facebook and Yahoo! sell advertising space to companies, serving adverts to the millions of users that these sites see every day.

Services such as Facebook, and Google are made available to users for free. Increasingly, such sites track the activity of users and analyse, or 'mine,' the data to build profiles. These are then used to present 'targeted' adverts aimed at the interests of specific users.

The success of this model of free services powered by targeted advertising has led Google to its $50 billion annual revenue, and caused Facebook to be valued at $104 billion when it first floated on the stock market in mid-2012.

Cloud computing

As the internet develops, new approaches to computing are emerging. Perhaps the most significant of these is the rise of *cloud computing*.

Rather than storing information on their home or business computers, or buying and updating software, the cloud lets users put all their data on internet servers and run their programs remotely. Outsourcing of functions in this way allows large *cloud providers* to maintain dedicated and large scale data centers as the physical presence of cloud computing. These data centers are dedicated locations in which large banks of computers can be centrally managed, connected to extremely high-speed internet connections, with significant power requirements.

Cloud computing offers significant cost and efficiency advantages, but also comes with risks: private or secret data stored in the cloud is an attractive target for hackers; if a company's internet connection goes down, they may be unable to access their data or conduct business; if the cloud computing service itself goes offline, or is attacked by hackers, any businesses or individuals that use it are affected.

ANNEX FIVE: METHODOLOGY

Methodology adopted by the expert group

At its first session, held from 17 to 21 January 2011, the open-ended intergovernmental expert group on cybercrime adopted a 'Methodology for the study':[1]

1. In order to achieve the mandate of the expert group regarding the study, the structure set out below has been elaborated to facilitate the conduct of the study, which will be carried out under the auspices of the expert group.

2. Each country will have the right to present its views, which should be reflected in the study.

3. The United Nations Office on Drugs and Crime (UNODC) will be tasked with developing the study, including developing a questionnaire, collecting and analysing data and developing a draft text of the study. To accomplish this task, UNODC will draw upon its internal expertise and capacity from across the various thematic branches of UNODC (Division for Treaty Affairs, Policy and Research Branch). For that purpose, adequate extrabudgetary resources should be made available to enable UNODC to discharge these functions efficiently. In order to help the Secretariat ensure that major technological expertise, systems and needs are adequately represented, each regional group will provide to the Secretariat names of governmental experts (not more than six), their contact information and their areas of expertise. The Secretariat will consult with the experts as a resource on an ad hoc basis, as appropriate.

4. The Secretariat will regularly brief and consult the Bureau of the expert group on the process and circulate to Member States the minutes of the consultations. The development of the list of experts is not intended to create any closed-ended expert group or other parallel or subsidiary bodies of the expert group.

5. For the information-gathering, UNODC will prepare a questionnaire for further dissemination to Member States, intergovernmental organizations and private sector entities (see the indicative timeline below), which will consist of a single survey instrument based on the outlines contained in the concept/working paper of the first meeting of the expert group, as amended, and on the recommendations of the first meeting of the expert group, as reflected in its report.

6. Secondarily, and as needed, the Secretariat, bearing in mind the need to have balanced representation of different regions, will consult with representatives from the private sector, including representatives of Internet service providers, users of services and other relevant actors; representatives from academia, from both developed and developing countries; and representatives from relevant intergovernmental organizations.

[1] E/CN.15/2011/19

Actions undertaken

This methodology was followed through the actions undertaken below:

17 to 21 January 2011	Adoption of the 'Collection of topics for consideration in a comprehensive study on impact of and response to cybercrime' and 'Methodology for the study and indicative timeline' by the first session of the open-ended intergovernmental expert group on cybercrime
14 September 2011	Decision of the Bureau to revise the indicative timeline due to phasing of the availability of funding for the Study, and to circulate a draft questionnaire prepared by the Secretariat in English only to all Member States for comment by 31 October 2011.
23 September 2011	Draft questionnaire sent to all Member States for comment by note verbale CU 2011/168.
10 October to 16 November 2011	Written comments on the questionnaire received from 18 Member States and incorporated by the Secretariat to the furthest extent possible.
19 January 2012	Finalized questionnaire approved by the Bureau.
29 February 2012	Questionnaire sent in six official languages to all Member States by note verbale CU 2012/19 for completion by 31 May 2012. Member States invited to also nominate specific private sector organizations or academic institutions to receive the Study questionnaire. Invitations to private sector organizations, academic organizations, and intergovernmental organizations to complete the Study questionnaire transmitted.
15-19 April 2012	Regional workshop in support of the Study held in Nairobi, Kenya, attended by 10 countries from Africa and one intergovernmental organization.
24-27 April 2012	Regional workshop in support of the Study held in Lebanon, Beirut, attended by 12 countries from Western Asia and Northern Africa and two intergovernmental organizations.
5-10 May 2012	Regional workshop in support of the Study held in Bangkok, Thailand, attended by 11 countries from Asia and one intergovernmental organization.
11 May 2012	Reminder note verbale CU 2012/102 concerning Study questionnaire sent to all Member States.
6 June 2012	Reminder note verbale CU 2012/117 concerning Study questionnaire sent to all Member States. Questionnaire completion deadline extended to 30 June 2012.
13 September 2012	Secretariat report to Extended Bureau on status of responses to the questionnaire, and deliberation of the Extended Bureau as to next steps.
1 October 2012	Preview of information on relevant legislation to be used by the Secretariat in analysis and drafting sent to all Member States by note verbale CU 2012/176 with invitation for comments and corrections to be submitted by 9 November 2012.
24 October 2012	Subsequent to Extended Bureau meeting of 13 September 2012, Decision of the Chair of the open-ended intergovernmental expert group on cybercrime to convene the second session of expert group in the week commencing 25 February 2013.
24 October to 30 January 2013	Written comments on legislation received from 16 Member States.
9 November 2012	Preliminary Study results sent to experts nominated by the regional groups.
6 December to 14 January 2013	Written comments on preliminary Study results received from four experts nominated by the regional groups.
30 January 2013	Executive summary of the comprehensive study on cybercrime sent to participants registered for the second session of the open-ended intergovernmental expert group on cybercrime.
8 February 2013	Full draft comprehensive study on cybercrime sent to participants registered for the second session of the open-ended intergovernmental expert group on cybercrime.
25 to 28 February 2013	Second session of the open-ended intergovernmental expert group on cybercrime.

Information gathered

Sixty-nine country responses to the questionnaire were received from Member States with the following geographical distribution:

Africa	Eastern Africa	2
	Northern Africa	4
	Southern Africa	3
	Western Africa	2
	TOTAL	11
Americas	Caribbean	2
	Central America	1
	North America	2
	South America	8
	TOTAL	13
Asia	Eastern Asia	3
	South-Eastern Asia	4
	Southern Asia	4
	Western Asia	8
	TOTAL	19
Europe	Eastern Europe	8
	Northern Europe	6
	Southern Europe	4
	Western Europe	6
	TOTAL	24
Oceania	Oceania	2
	TOTAL	2

Over 1500 private sector, 380 academic, and 80 intergovernmental organizations were invited directly, in accordance with the Study methodology, by the Secretariat to contribute information for the study. Private sector organizations were identified with equitable geographical distribution through United Nations Global Compact, ITU, and industry association memberships. Academic organizations were identified through a list of world top 500 universities. Forty private sector, 16 academic, and 11 intergovernmental organizations responded to the Study questionnaire, or completed a telephone interview based on the Study questionnaire:

Private sector organizations	Academic organizations
Accenture	B-Ccentre
Aconite Internet Solutions Ltd.	Beijing Normal University
Admiral Insurance Company	Brown University
Allen & Overy LLP	Eberhard Karls University, Tübingen
Betterley Risk Consultants, Inc.	International Association of IT Lawyers
Casdisa de Promociones, S.A.	Masaryk University
Cisco Systems, Inc.	National Institute of Communication Technologies
Cooperativa La Cruz Azul S.C.L.	Norwegian Police University College
Danfoss A/S	Royal Melbourne Institute of Technology
Digicel Group Ltd.	University of Adelaide

Ernst & Young Global Limited	University of Durham
Estudio de Informática Forense	University of Erlangen-Nuremberg
FIRST.org, Inc.	University of Lausanne
Gloria Group	Vrije Universiteit Brussel
Hewlett-Packard Company	Waseda University/School of Law
Hogan Lovells	Xi'an Jiaotong University
Huawei Technologies Co., Ltd.	**Intergovernmental organizations**
I2 Integrity International	Council of Europe
InfoCom Research, Inc.	European Union
International Cyber Security Protection Alliance	FAO
Internet Security Alliance	IFAD
ID Experts Corp.	INTERPOL
Juniper Networks, Inc.	OSCE
KPMG International Cooperative	UNCTAD
Logica Pvt Ltd	UNDP
McKinsey & Company, Inc.	UNHCR
Mitsubishi UFJ Financial Group, Inc.	UNICRI
Nippon Telegraph and Telephone Corporation	UNWomen
OSDE Organización de Servicios Directos Empresarios	
Palantir Technologies, Inc.	
PricewaterhouseCoopers	
Superintendencia de Telecomunicaciones (Supertel)	
Symantec Corporation	
Team Cymru, Inc.	
Threatmetrix Inc.	
Trend Micro Inc.	
Trustwave	
Verizon Communications Inc.	
Vodafone Group Plc.	
WISeKey SA	

Results from responses to the Study questionnaire are presented in the Study in aggregate format, either representing all available responses to a particular question, or presented by region, or by country development level. Due to the low number of responses from Oceania, regions used are: 'Europe', 'Asia and Oceania', 'Americas', and 'Africa'.[2]

Most figures present the 'percentage of respondents' that selected a particular response option. In cases where multiple response options were allowed, percentages are calculated either according to the total number of countries that answered that particular question ('n'), or according to the total number of answer choices selected ('r'). The values 'n' and 'r' (as required) are indicated in all figure source notes. Thus, where 'n' is used as the basis for calculations in such questions, the presented results may sum to more than 100 per cent.

Many questions in the Study questionnaire allowed for both a 'drop-down' selection and additional 'free text' answers or clarifications. In such cases, all information provided in free text answers or clarifications was analysed, and the data coded as appropriate, in order to integrate free text responses with drop-down answers. In some cases, this resulted in the addition of new response categories in the results figures.

Where figures made use of quantitative data supplied by respondents, this is frequently presented using relevant denominator data, including, as appropriate, the total number of internet users in a country, or

[2] Geographical regions used are as defined by the United Nations Statistics Division at http://unstats.un.org/unsd/methods/m49/m49regin.htm

the total number of law enforcement personnel. Some figures further make use of disaggregation by level of country development.[3] Where quantitative data is aggregated, values presented correspond to medians, with lower and upper quartiles indicated by the use of additional bars.

[3] Sources used include: World Bank Development Indicators incorporation ITU World Telecommunication/ICT Indicators (number of internet users, by country); UNDP Human Development Index (human development); United Nations Survey of Crime Trends and Operations of Criminal Justice Systems (number of law enforcement and criminal justice personnel and number of recorded offences and suspects for homicide and rape).

Page left intentionally blank

UNODC

United Nations Office on Drugs and Crime

Vienna International Centre, PO Box 500, 1400 Vienna, Austria
Tel: (+43-1) 26060-0, Fax: (+43-1) 26060-5866, www.unodc.org

Printed in Austria
V.13-80699—February 2013—300